comnet
Communication Networks

INSTALLATION AND OPERATION MANUAL

# CNGE24MS

## ENVIRONMENTALLY HARDENED MANAGED ETHERNET SWITCH WITH (8) 100/1000BASE-FX & (16) GIGABIT COMBO PORTS

v1.4 February 25, 2013

The ComNet™ CNGE24MS has eight 100/1000Base-FX SFP ports and sixteen Gigabit combo ports that allow for TX or FX transmission. All SFP ports utilize ComNet Small Form Factor (SFP) pluggable modules for the selection of fiber and connector type and distance. The IEEE802.3-compliant unit offers multiple Ethernet redundancy protocols (ComRing, C-Ring, and MSTP/RSTP/STP) which protect your applications from network interruptions or temporary malfunctions by redirecting transmission within the network. The switch provides advanced IP-based management that can limit the maximum bandwidth for each connected IP device, allowing the user to adjust usage. Application-based QoS can set a higher priority for data streaming. The Device-Binding function can prevent unauthorized network access, increasing security. The unit also provides advanced DOS/DDOS auto prevention. If IP flow becomes too large, too quickly, the switch will lock the source IP address for a set period preventing unauthorized access. The switch offers centralized and convenient management and is also configurable by Web-based Telnet, and Console (CLI) configurations.

# Contents


Regulatory Compliance Statement 3

Warranty 3

Disclaimer 3

Safety Indications 3

Overview 4

- Introduction 4
- Software Features 5
- Hardware Features 6

Hardware Overview 7

- Front Panel 7
- Rear Panel 8
- Rack mount kit assembly 9
- Front Panel LEDs 10

Cables 11

- Ethernet Cables 11
- 10/100/1000BASE-T(X) Pin Assignments 11
- SFP 13
- Console Cable 14

WEB Management 16

- Configuration by Web Browser 16
- About Web-based Management 16

Command Line Interface Management 92

About CLI Management 92

Technical Specifications 105

# Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

# Warranty

ComNet warrants that all ComNet products are free from defects in material and workmanship for a specified warranty period from the invoice date for the life of the installation. ComNet will repair or replace products found by ComNet to be defective within this warranty period, with shipment expenses apportioned by ComNet and the distributor. This warranty does not cover product modifications or repairs done by persons other than ComNet-approved personnel, and this warranty does not apply to ComNet products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

# Disclaimer

Information in this publication is intended to be accurate. ComNet shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ComNet reserves the right to revise the contents of this publication without notice.

# Safety Indications

» The equipment can only be accessed by trained ComNet service personnel.

» This equipment should be installed in secured location.

# Overview

## Introduction

The CNGE24MS series are managed redundant ring Ethernet switches with 16xGigabit combo ports and 8x100/1000Base-X SFP ports. With complete support of Ethernet Redundancy protocol, C-Ring (recovery time <20ms over 250 units of connection) and MSTP/RSTP/STP (IEEE IEEE 802.1s/w/D) can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. ComNet switches provide advanced and IP-based bandwidth management that can limit the maximum bandwidth for each IP device. The user can configure IP camera and NVR with more bandwidth and limit other device bandwidth. ComNet's switch series also support application-based QoS. Application-based QoS can set highest priority for data stream according to TCP/UDP port number. And all functions of CNGE24MS can also be managed centralized and convenient by e-Console, as well as the Web-based interface, Telnet and console (CLI) configuration. Therefore, the switch is one of the most reliable choice for highly-managed and Gigabit Fiber Ethernet applications.

## Software Features

» Fastest Redundant Ethernet Ring (Recovery time <20ms over 250 units connection)
» Supports Ring Coupling, Dual Homing, and RSTP-over-Ring
» Supports SNMPv1/v2/v3 & RMON & Port base/IEEE 802.1Q VLAN Network Management
» Event notification by Email, SNMP trap and Relay Output
» Web-based, Telnet, and Console (CLI) configuration
» Enable/disable ports, MAC based port security
» Port-based network access control (IEEE 802.1x)
» VLAN (IEEE 802.1q) to segregate and secure network traffic
» RADIUS centralized password management
» SNMPv3 encrypted authentication and access security
» RSTP (IEEE 802.1w)
» Quality of Service (IEEE 802.1p) for real-time traffic
» VLAN (IEEE 802.1q) with support for double-tagging and GVRP
» IGMP Snooping for multicast filtering
» Port configuration, status, statistics, mirroring, and security
» Remote Monitoring (RMON)

## Hardware Features

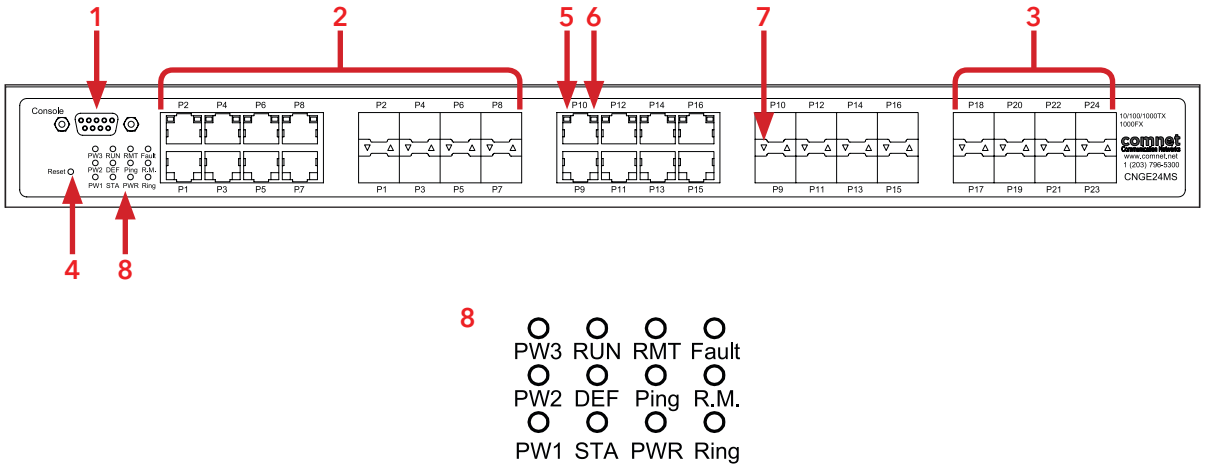
» 3 × Redundant power inputs
» Operating Temperature: -40 to 75°C
» Storage Temperature: -40 to 85°C
» Operating Humidity: 5% to 95%, non-condensing
» Casing: IP-30 Aluminum
» 16 × Combo ports with 10/100/1000Base-T(X) and 100/1000Base-X SFP
» 8 × 100/1000Base-X SFP ports
» Console Port
» Dimensions (W × D × H): 431 × 342 × 44 mm

# Hardware Overview

## Front Panel

The following table describes the labels that are affixed to the CNGE24MS.

| Port | Description |
|---|---|
| SFP ports | 16 × 100/1000BaseX on SFP port(combo) &<br>8 × 100/1000BaseX on SFP port |
| Giga Ethernet Port | 16 × 10/100/1000Base-T (combo) |
| Console | Use RS-232 with DB9 connecter to manage switch. |







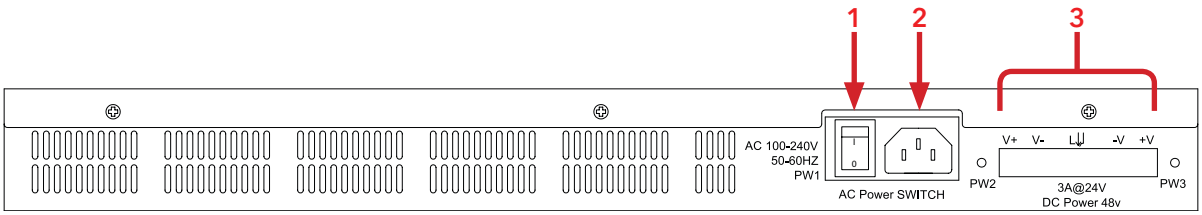
*CNGE24MS Front Panel*

1. Console port (DB9)
2. 10/100/1000Base-T(X) Ethernet port and 100/1000Base-X SFP (combo port)
3. 100/1000Base-X Fiber port on SFP
4. Reset button: Push the button 3 seconds for reset; 5 seconds for factory default.
5. LED for Ethernet ports 1000Mbps Link/Act status
6. LED for Ethernet ports 10/100Mbps Link/Act status
7. LED for SFP ports Link/Act status
8. Front Panel LED Status:
   - » LED for PW1: When the PWR1 links, the green LED will be light on.
   - » LED for PW2: When the PWR2 links, the green LED will be light on.
   - » LED for PW3: When the PWR3 links, the green LED will be light on.

- LED for STA: Green: Indicates that the system ready. The LED is blinking when the system is upgrading firmware
- LED for PWR: This LED lights on when the power module is activated.
- LED for R.M. (Ring master): When the LED lights on, this switch is designated as the ring master of the Ring topology.
- LED for Ring: When the LED light on, the C-Ring is activated.
- LED for DEF: System resets to default configuration.
- LED for Ping: System is processing "PING" request.
- LED for RUN: System is operating continuously.
- LED for RMT: System is accessed remotely.
- LED for Fault: Indicates unexpected event occurred.

## Rear Panel

The rear panel of CNGE24MS is displayed as below:




*CNGE24MS Rear Panel*

1. Power Switch
2. Power input for AC 100V~240V / 50~60Hz.
3. Power input for DC 36~72V and fault relay output

## Rack mount kit assembly

You can find the rack-mount kit and the screws in the packing box. Please assemble the rack-mount kit on the switch with screws as shown below:

# Front Panel LEDs

## LED indicators

| LED | Color | Status | Description |
|---|---|---|---|
| PW1 | Green | On | PWR1 linked |
| PW2 | Green | On | PWR2 linked |
| PW3 | Green | On | PWR3 linked |
| STA | Green | On | The power module is in PWR UP state |
| | | Blinking | The system is upgrading firmware |
| DEF | Green | On | System resets to default configuration |
| RUN | Green | Slowly blinking | System is operating continuously |
| PWR | Green | On | DC power module activated |
| Ping | Green | Blinking | System is processing “PING” request |
| RMT | Green | Blinking | System is accessed remotely |
| Ring | Green | On | Ring enabled |
| | | Slowly blinking | Ring has only One link (lacks one link to build the ring) |
| | | Fast blinking | Ring working normally |
| R.M | Green | On | The system is operating in C-Ring Master mode |
| Fault | Amber | On | Unexpected event occurred. |
| **10/100/1000Base-T(X) Gigabit Ethernet ports** | | | |
| LINK/ ACT | Green | On | Port speed 1000Mbps link up |
| | | Blinking | Data Transmitted at 1000Mbps |
| | Amber | On | Port speed 10/100Mbps link up |
| | | Blinking | Data Transmitted at 10/100Mbps |
| **SFP** | | | |
| LINK/ ACT | Green | On | Port link up |
| | | Blinking | Data transmitted |

# Cables

## Ethernet Cables

The CNGE24MS switches have standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5, & 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

*Cable Types and Specifications*

| Cable | Type | Max. Length | Connector |
|---|---|---|---|
| 10BASE-T | Cat. 3, 4, 5 100Ω | UTP 100m (328ft) | RJ-45 |
| 100BASE-TX | Cat. 5 100Ω UTP | UTP 100m (328ft) | RJ-45 |
| 1000BASE-TX | Cat. 5/Cat. 5e 100Ω UTP | UTP 100m (328ft) | RJ-45 |

## 10/100/1000BASE-T(X) Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

*10/100 Base-T RJ-45 Pin Assignments*

| Pin Number | Assignment |
|---|---|
| 1 | TD+ |
| 2 | TD- |
| 3 | RD+ |
| 4 | Not used |
| 5 | Not used |
| 6 | RD- |
| 7 | Not used |
| 8 | Not used |

***Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.***

*1000 Base-T RJ-45 Pin Assignments*

| Pin Number | Assignment |
|---|---|
| 1 | BI_DA+ |
| 2 | BI_DA- |
| 3 | BI_DB+ |
| 4 | BI_DC+ |
| 5 | BI_DC- |
| 6 | BI_DB- |
| 7 | BI_DD+ |
| 8 | BI_DD- |

***Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.***

The CNGE24MS switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10/100BASE-T(X) MDI and MDI-X port pin-outs:

*10/100 Base-T MDI/MDI-X pin assignments*

| Pin Number | MDI port | MDI-X port |
|---|---|---|
| 1 | TD+ (transmit) | RD+ (receive) |
| 2 | TD- (transmit) | RD- (receive) |
| 3 | RD+ (receive) | TD+ (transmit) |
| 4 | Not used | Not used |
| 5 | Not used | Not used |
| 6 | RD- (receive) | TD- (transmit) |
| 7 | Not used | Not used |
| 8 | Not used | Not used |

***Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.***

*1000 Base-T MDI/MDI-X pin assignments*

| Pin Number | MDI port | MDI-X port |
|---|---|---|
| 1 | BI_DA+ | BI_DB+ |
| 2 | BI_DA- | BI_DB- |
| 3 | BI_DB+ | BI_DA+ |
| 4 | BI_DC+ | BI_DD+ |
| 5 | BI_DC- | BI_DD- |
| 6 | BI_DB- | BI_DA- |
| 7 | BI_DD+ | BI_DC+ |
| 8 | BI_DD- | BI_DC- |

***Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.***

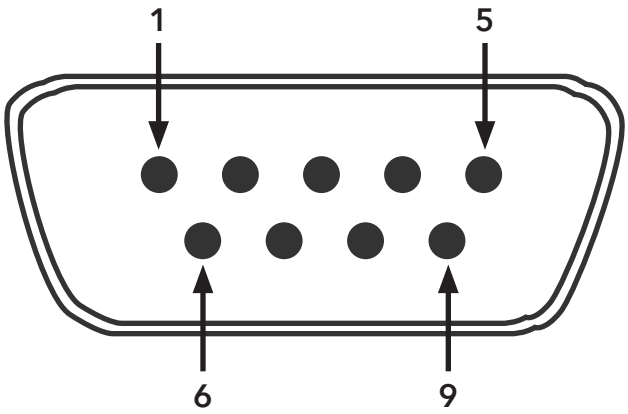
## SFP

The Switch has fiber optic ports that utilize SFP connectors. ComNet offers a wide selection of SFP modules that offer different fiber type, connector type and distances. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

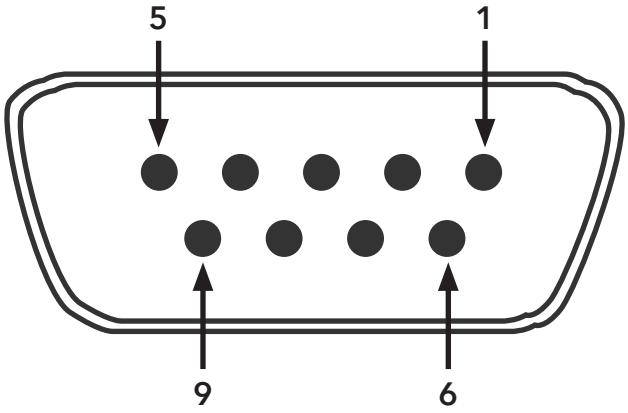
*Switch A* *Fiber Cord* *Switch B*

## Console Cable

Each CNGE24MS switch can be managed by its console port. You can connect them to PC via an RS-232 cable with DB-9 female connector.




*DB-9 Male*




*DB-9 Female*

| Pin | Male Connector | Female Connector |
|---|---|---|
| 1 | Received Line Signal Detect (Received by DTE Device) | Received Line Signal Detect (Transmitted from DCE Device) |
| 2 | Received Data (Received by DTE Device) | Transmitted Data (Transmitted from DCE Device) |
| 3 | Transmitted Data (Transmitted from DTE Device) | Received Data (Received by DCE Device) |
| 4 | DTE Ready (Transmitted from DTE Device) | DTE Ready (Received by DCE Device) |
| 5 | Signal Ground | Signal Ground |
| 6 | DCE Ready (Received by DTE Device) | DCE Ready (Transmitted from DCE Device) |
| 7 | Request to Send (Transmitted from DTE Device) | Clear to Send (Received by DCE Device) |
| 8 | Clear to Send (Received by DTE Device) | Request to Send (Transmitted from DCE Device) |
| 9 | Ring Indicator (Received by DTE Device) | Ring Indicator (Transmitted from DCE Device) |

# WEB Management

*Attention: While installing and upgrading firmware, please remove physical loop connection first. DO NOT power off equipment while the firmware is upgrading!*

## Configuration by Web Browser

This section provides instruction on configuration through the Web browser.

## About Web-based Management

An embedded HTML web site resides in the flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It utilizes Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

*Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.*

### Preparing for Web Management

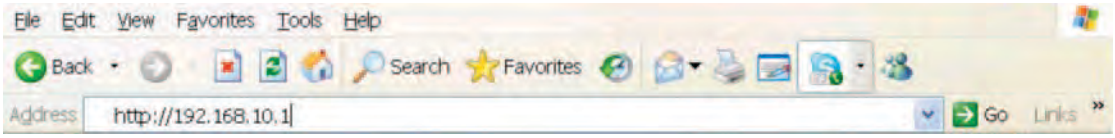
The default value is as below:

IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.254
User Name: admin
Password: admin

## System Login

1. Launch your Web Browser.

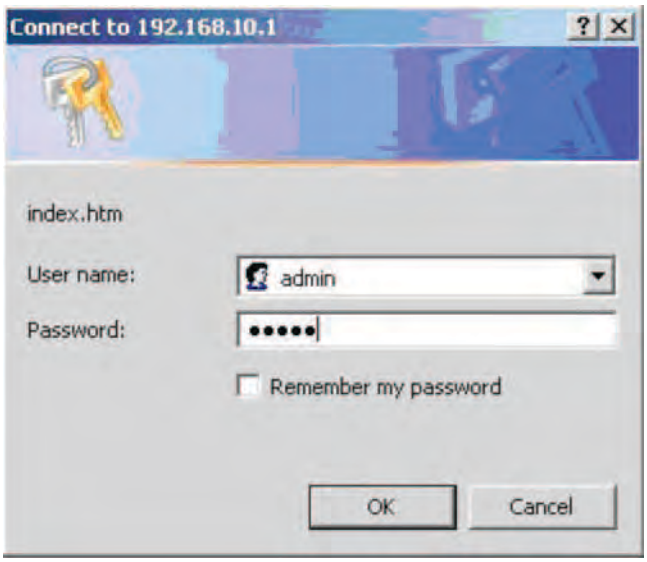
2. Type http:// and the IP address of the switch. Press **Enter**.




3. The login screen appears.

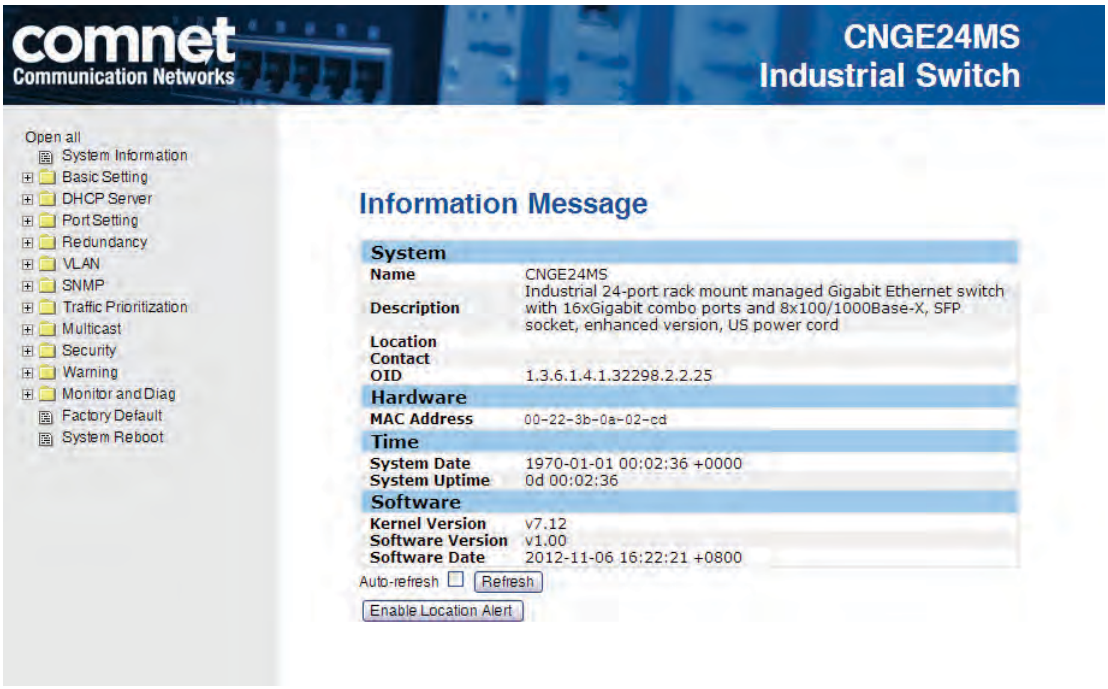
4. Enter username and password. The default username and password is **admin**.

5. Select **Enter** or **OK** button, then the main interface of the Web-based management appears.




*Login screen*

Main Interface

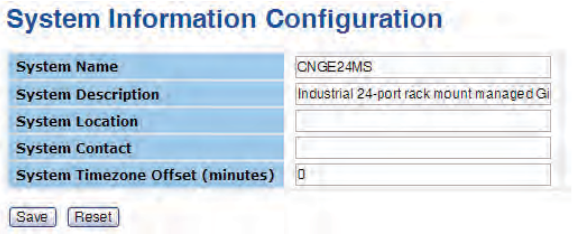



*Main interface*

## Basic Setting

### System Information

The switch system information is provided here.




*System Information interface*

| Label | Description |
|---|---|
| System Name | The administrator-assigned name for this managed node. By convention, this is the node's fully qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alphabet character, and the first or last character must not be a minus sign. The allowed string length is 0 to 255. |
| System Description | The administrator-assigned description for this managed node. The allowed string length is 0 to 255, and the allowed contents are the ASCII characters from 32 to 126. |
| System Location | The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed contents are the ASCII characters from 32 to 126. |
| System Contact | The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed contents are the ASCII characters from 32 to 126. |
| Timezone Offset | Enter the name of contact person or organization<br>Provide the time zone offset relative to UTC/GMT.<br>The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

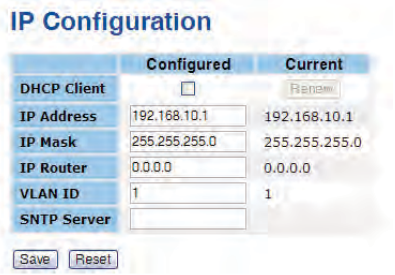
### Admin & Password

This page allows you to configure the system password that is required to access the web pages or log in from CLI.

| Label | Description |
|---|---|
| Old Password | Enter the current system password. If this is incorrect, the new password will not be set. |
| New Password | The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126. |
| Confirm password | Re-type the new password. |
| Save | Select to save changes. |

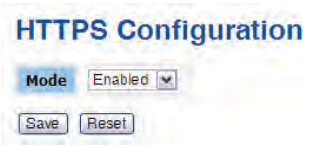
## IP Setting

Configure the switch-managed IP information on this page.



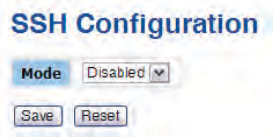

| Label | Description |
|---|---|
| DHCP Client | Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup. |
| IP Address | Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.10.1 |
| IP Mask | Assign the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask |
| IP Router | Assign the network gateway for the switch. The default gateway is 192.168.10.254 |
| VLAN ID | Provide the managed VLAN ID. The allowed range is 1 through 4095. |
| SNTP Server | SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |
| Renew | Select to renew DHCP. This button is only available if DHCP is enabled. |

## HTTPS




| Label | Description |
|---|---|
| Mode | Indicates the HTTPS mode operation. Possible modes are:<br>Enabled: Enable HTTPS mode operation.<br>Disabled: Disable HTTPS mode operation. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

## SSH

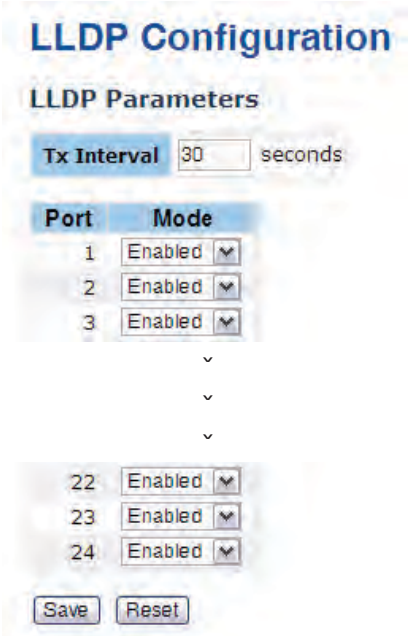



| Label | Description |
|---|---|
| Mode | Indicates the SSH mode operation. Possible modes are:<br>Enabled: Enable SSH mode operation.<br>Disabled: Disable SSH mode operation. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

## LLDP

LLDP Parameters

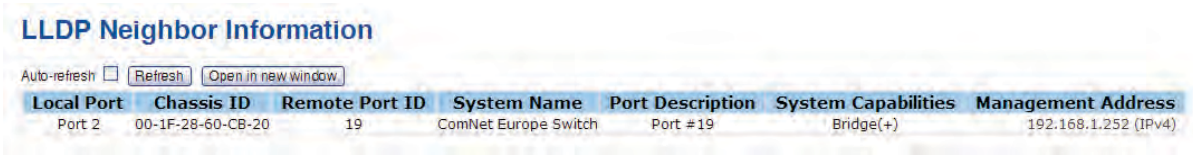
This page allows the user to inspect and configure the current LLDP port settings.




| Label | Description |
|---|---|
| TX Interval | The switch periodically transmits LLDP frames to its neighbors for keeping the network discovery information up-to-date. The interval between each LLDP frame is determined by the TX Interval value. Valid values are restricted to 5 - 32768 seconds. |
| Port | The switch port number of the logical LLDP port. |
| Mode | Enable or Disable LLDP |

## LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

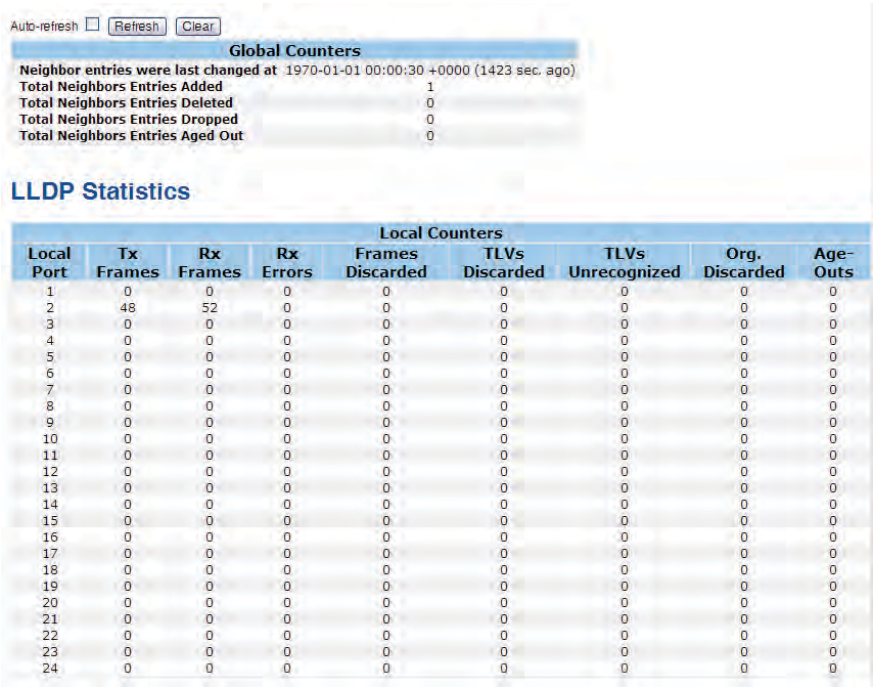



| Label | Description |
|---|---|
| Local Port | The port on which the LLDP frame was received. |
| Chassis ID | The Chassis ID is the identification of the neighbor's LLDP frames. |
| Remote Port ID | The Remote Port ID is the identification of the neighbor port. |
| System Name | System Name is the name advertised by the neighbor unit. |
| Port Description | Port Description is the port description advertised by the neighbor unit. |
| System Capabilities | System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:<br>1. Other<br>2. Repeater<br>3. Bridge<br>4. WLAN Access Point<br>5. Router<br>6. Telephone<br>7. DOCSIS cable device<br>8. Station only<br>9. Reserved<br>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-). |
| Management Address | Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address. |
| Refresh | Select to refresh the page immediately. |
| Auto-Refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

## LLDP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole network of switches, while local counters refer to counters for the currently selected switch.



Auto-refresh Refresh Clear

| Global Counters | |
|---|---|
| Neighbor entries were last changed at | 1970-01-01 00:00:30 +0000 (1423 sec. ago) |
| Total Neighbors Entries Added | 1 |
| Total Neighbors Entries Deleted | 0 |
| Total Neighbors Entries Dropped | 0 |
| Total Neighbors Entries Aged Out | 0 |

LLDP Statistics

| Local Counters | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 48 | 52 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

### Global Counters

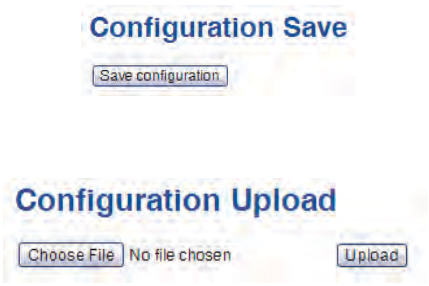
| Label | Description |
|---|---|
| Neighbor entries were last changed at | Shows the time for when the last entry was last deleted or added. It is also shows the time elapsed since last change was detected. |
| Total Neighbors Entries Added | Shows the number of new entries added since switch reboot. |
| Total Neighbors Entries Deleted | Shows the number of new entries deleted since switch reboot. |
| Total Neighbors Entries Dropped | Shows the number of LLDP frames dropped due to the entry table being full. |
| Total Neighbors Entries Aged Out | Shows the number of entries deleted due to Time-To-Live expiring. |

## Local Counters

| Label | Description |
|---|---|
| Local Port | The port on which LLDP frames are received or transmitted. |
| TX Frames | The number of LLDP frames transmitted on the port. |
| Rx Frames | The number of LLDP frames received on the port. |
| Rx Errors | The number of received LLDP frames containing some kind of error. |
| Frames Discarded | If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out. |
| TLVs Discarded | Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded. |
| TLVs Unrecognized | The number of well-formed TLVs, but with an unknown type value. |
| Org. Discarded | The number of organizationally TLVs received. |
| Age-Outs | Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented. |
| Refresh | Select to refresh the page immediately. |
| Clear | Clears the local counters. All counters (including global counters) are cleared upon reboot. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

### Backup/Restore Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags.



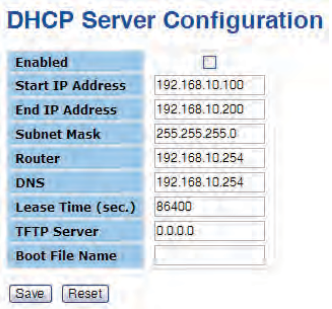

### Firmware Update

This page facilitates an update of the firmware controlling the switch.

### DHCP Server

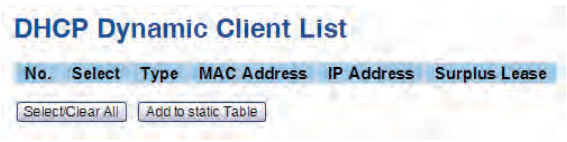
### Setting

The system provides DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.



### DHCP Dynamic Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display in here.



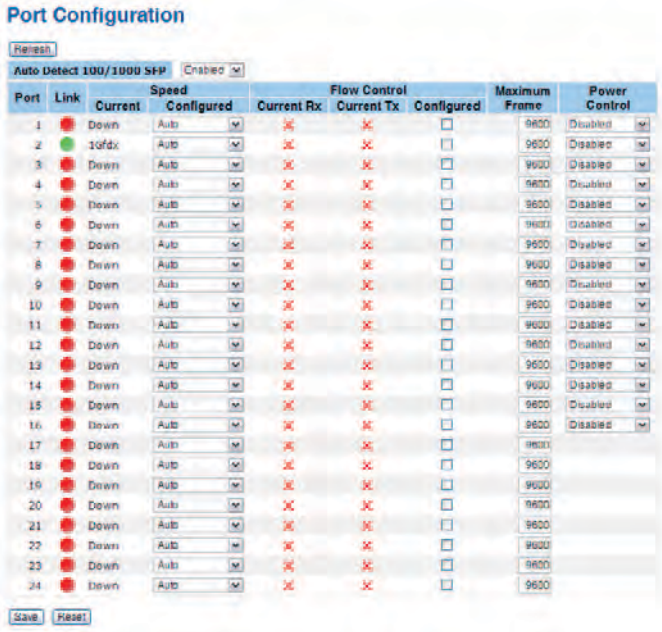

### DHCP Client List

You can assign the specific IP address that is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.

### Port Setting

### Port Control

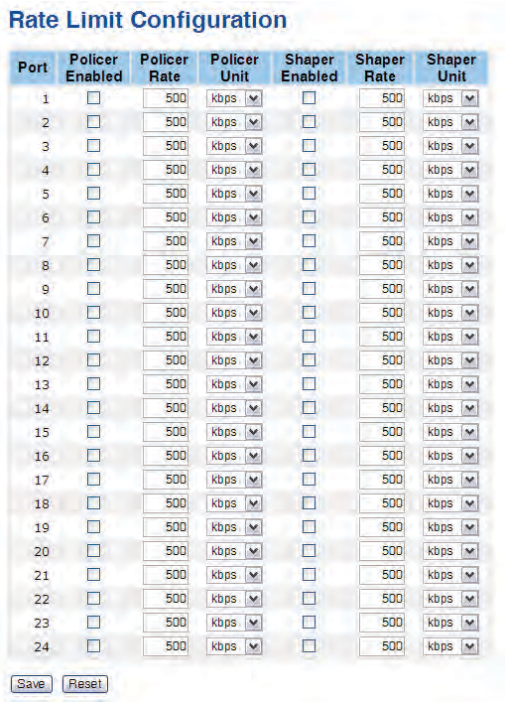
This page displays current port configurations. Ports can also be configured here.



| Label | Description |
|---|---|
| Port | This is the logical port number for this row. |
| Link | The current link state is displayed graphically. Green indicates the link is up and red that it is down. |
| Current Link Speed | Provides the current link speed of the port. |
| Configured Link Speed | Select any available link speed for the given switch port.<br>Auto Speed: Selects the highest speed that is compatible with a link partner.<br>Disabled: Disables the switch port operation. |
| Flow Control | When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner.<br>When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current TX column indicates whether pause frames on the port are transmitted. The Rx and TX settings are determined by the result of the last Auto-Negotiation.<br>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed. |
| Maximum Frame | Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes. |
| Power Control | The column allows for changing the power savings mode parameters per port.<br>Disabled: All power savings mechanisms disabled.<br>ActiPHY: Link down power savings enabled.<br>Perfect-Reach: Link up power savings enabled.<br>Enabled: Both link up and link down power savings enabled. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |
| Refresh | Select to refresh the page. Any changes made locally will be undone. |

## Rate Limit

Configure the switch port rate limit for Policers and Shapers on this page.

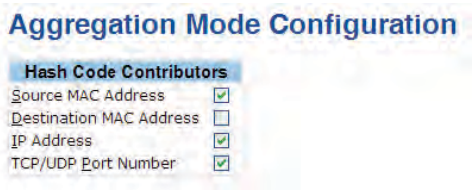



| Label | Description |
|---|---|
| Port | The logical port for the settings contained in the same row. |
| Policer Enabled | Enable or disable the port policer. The default value is “Disabled”. |
| Policer Rate | Configure the rate for the port policer. The default value is “500”. This value is restricted to 500-1000000 when the “Policer Unit” is “kbps,” and it is restricted to 1-1000 when the “Policer Unit” is “Mbps” |
| Policer Unit | Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is “kbps.” |
| Shaper Enabled | Enable or disable the port shaper. The default value is “Disabled.” |
| Shaper Rate | Configure the rate for the port shaper. The default value is “500.” This value is restricted to 500-1000000 when the “Policer Unit” is “kbps,” and it is restricted to 1-1000 when the “Policer Unit” is “Mbps” |
| Shaper Unit | Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is “kbps.” |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

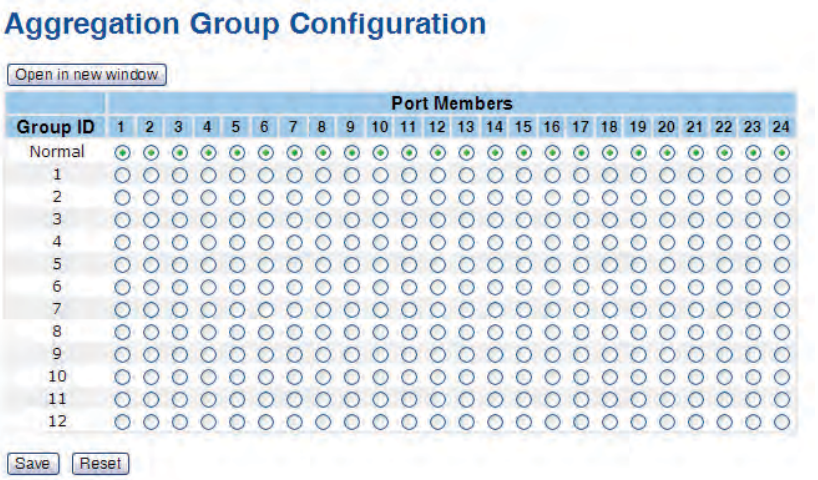
## Port Trunk

### Trunk Configuration

This page is used to configure the Aggregation hash mode and the aggregation group.



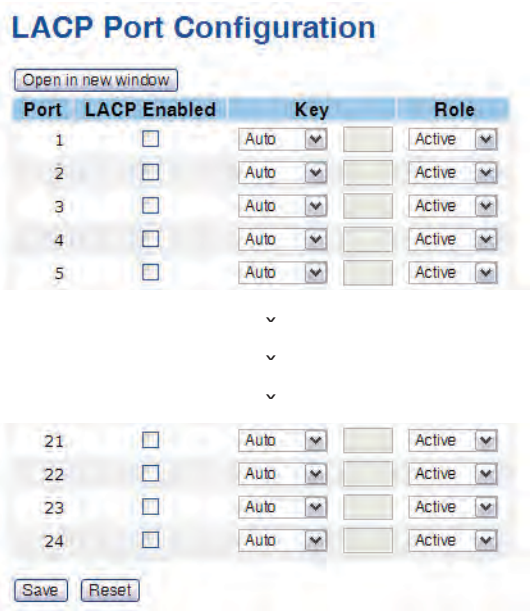

| Label | Description |
|---|---|
| Source MAC Address | The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled. |
| Destination MAC Address | The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled. |
| IP Address | The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled. |
| TCP/UDP Port Number | The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled. |




| Label | Description |
|---|---|
| Group ID | Indicates the group ID for the settings contained in the same row. Group ID “Normal” indicates there is no aggregation. Only one group ID is valid per port. |
| Port Members | Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group. |

## LACP Port Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well.




| Label | Description |
|---|---|
| Port | Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port. |
| LACP Enabled | Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group. |
| Key | The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. |
| Role | The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to). |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

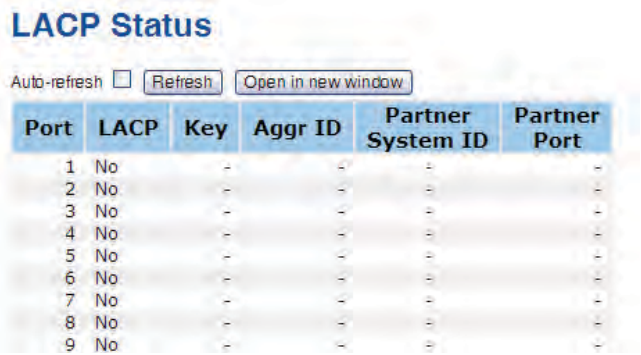
## LACP System Status

This page provides a status overview for all LACP instances.

| Label | Description |
|---|---|
| Aggr ID | The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id' |
| Partner System ID | The system ID (MAC address) of the aggregation partner. |
| Partner Key | The Key that the partner has assigned to this aggregation ID. |
| Last Changed | The time since this aggregation changed. |
| Local Ports | Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port". |
| Refresh | Select to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

## LACP Status

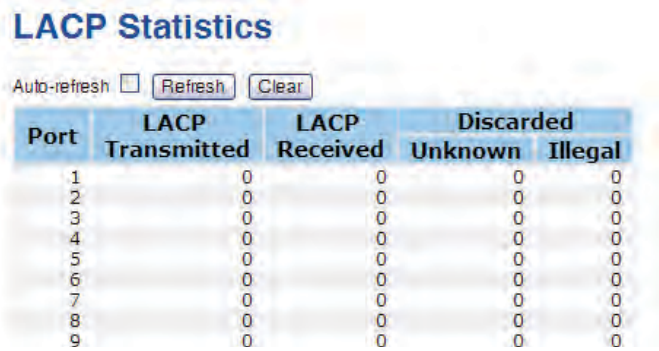
This page provides a status overview for LACP status for all ports.


LACP Status
Auto-refresh
Refresh
Open in new window
Port LACP Key Aggr ID Partner System ID Partner Port
1 No - - - -
2 No - - - -
3 No - - - -
4 No - - - -
5 No - - - -
6 No - - - -
7 No - - - -
8 No - - - -
9 No - - - -

| Label | Description |
|---|---|
| Port | The switch port number. |
| LACP | 'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled. |
| Key | The key assigned to this port. Only ports with the same key can aggregate together. |
| Aggr ID | The Aggregation ID assigned to this aggregation group. |
| Partner System ID | The partners System ID (MAC address). |
| Partner Port | The partners port number connected to this port. |
| Refresh | Select to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

### LACP Statistics

This page provides an overview for LACP statistics for all ports.

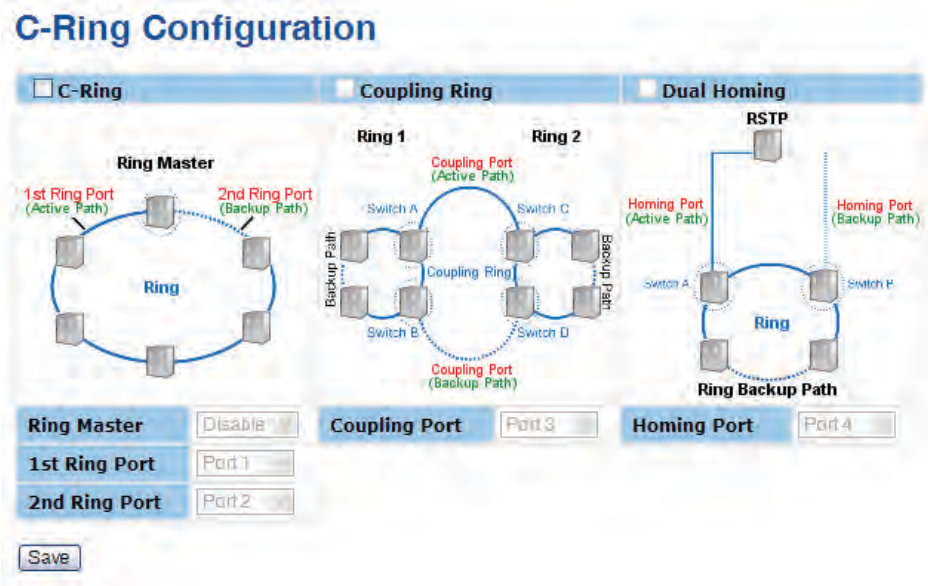



| Label | Description |
|---|---|
| Port | The switch port number |
| LACP Transmitted | Shows how many LACP frames have been sent from each port |
| LACP Received | Shows how many LACP frames have been received at each port. |
| Discarded | Shows how many unknown or illegal LACP frames have been discarded at each port. |
| Refresh | Select to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |
| Clear | Clears the counters for all ports |

## Redundancy

### C-Ring

C-Ring is the most powerful Ring in its class. The recovery time of C-Ring is less than 20 ms for Gigabit Ethernet switches. It can reduce unexpected damage caused by network topology change. C-Ring Supports 3 Ring topologies: C-Ring, Coupling Ring, and Dual Homing.



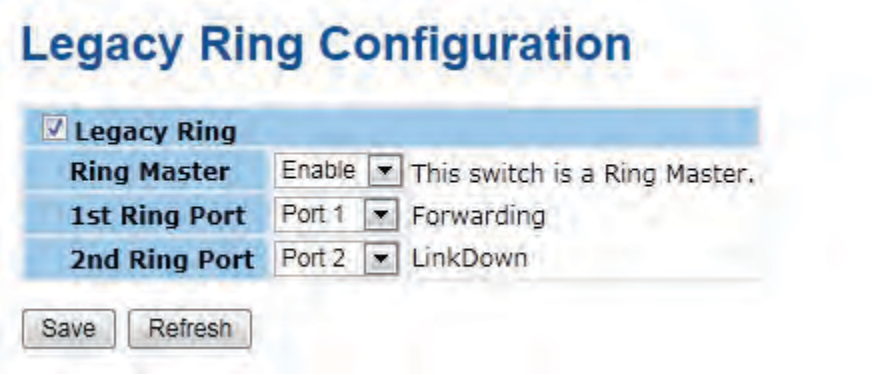

*Ring interface*

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| C-Ring | Mark to enable C-Ring. |
| Ring Master | There should be one and only one Ring Master in a ring. However if there are two or more switches that are set as Ring Masters, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters. |
| 1st Ring Port | The primary port, when this switch is C-Ring Master. |
| 2nd Ring Port | The backup port, when this switch is C-Ring Master. |
| Coupling Ring | Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings. |
| Coupling Port | Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link.<br>Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode. |
| Dual Homing | Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode. |
| Homing Port | Set a port as homing port. |
| Save | Select **Save** to set the configurations. |

***Note: We don't recommend that you set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.***

### Legacy Ring




Legacy ring provides support for the switch to be used in an existing ring of ComNet X-Ring enabled switches.

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring or Legacy Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch that one of its two member ports would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

The switch supports the function and interface for setting the switch as the ring master or not. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode can be enabled by setting the Legacy Ring configuration interface. Also, the user can identify whether the switch is the ring master by checking the R.M. LED indicator on the front panel of the switch.

| Label | Description |
|---|---|
| Legacy Ring | To enable the Legacy Ring (X-Ring) function, tick the checkbox beside the Legacy Ring label. If this checkbox is not ticked, all the ring functions are unavailable. |
| Ring Master | Select Enable for this switch to be the ring master or Disable for this switch to be a working switch. |
| 1st Ring Port | The primary port, when this switch is Ring Master. Select a port to assign from the pull down selection menu. |
| 2nd Ring Port | The backup port, used when this switch is Ring Master and the primary port fails. Select a port to assign from the pull down selection menu. |
| Save | Select to save changes. |
| Refresh | Select to refresh the page immediately. |

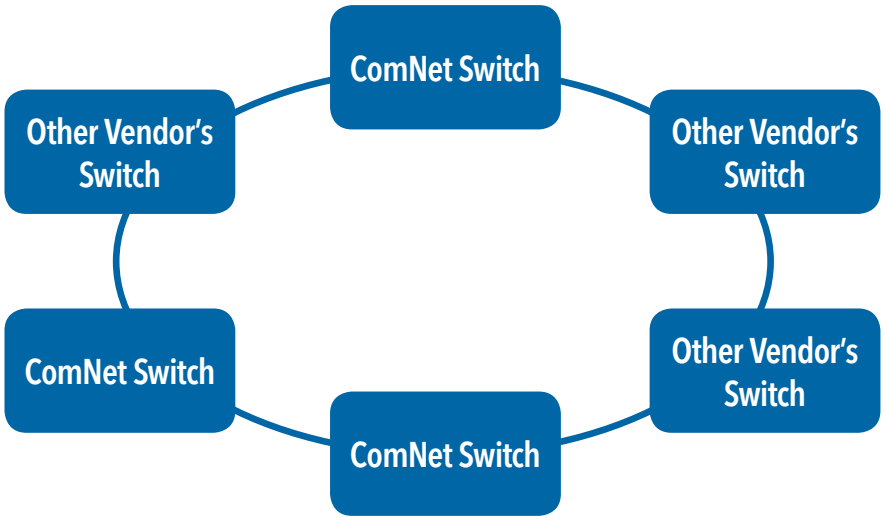
### COM-Ring

You can add ComNet switches into a network constructed by another ring technology and enable COM-Ring to cooperate with another vendor's managed switch.

*ComRing interface*

| Label | Description |
|---|---|
| Enable | Enable the COM-Ring function |
| Vendor | Select the vendor whose ring you want to join |
| 1st Ring Port | Select the port that connects to the ring |
| 2nd Ring Port | Select the port that connects to the ring |

The application of COM-Ring is shown as below.

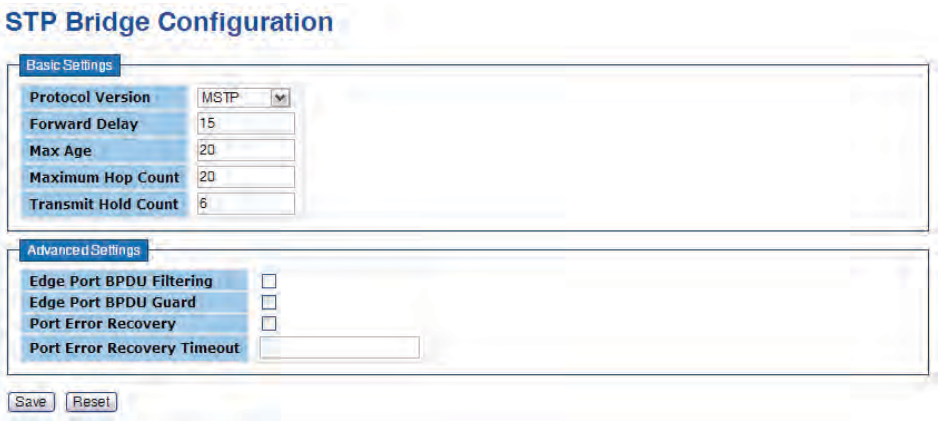



*COM-Ring connection*

## MSTP

### Bridge Settings

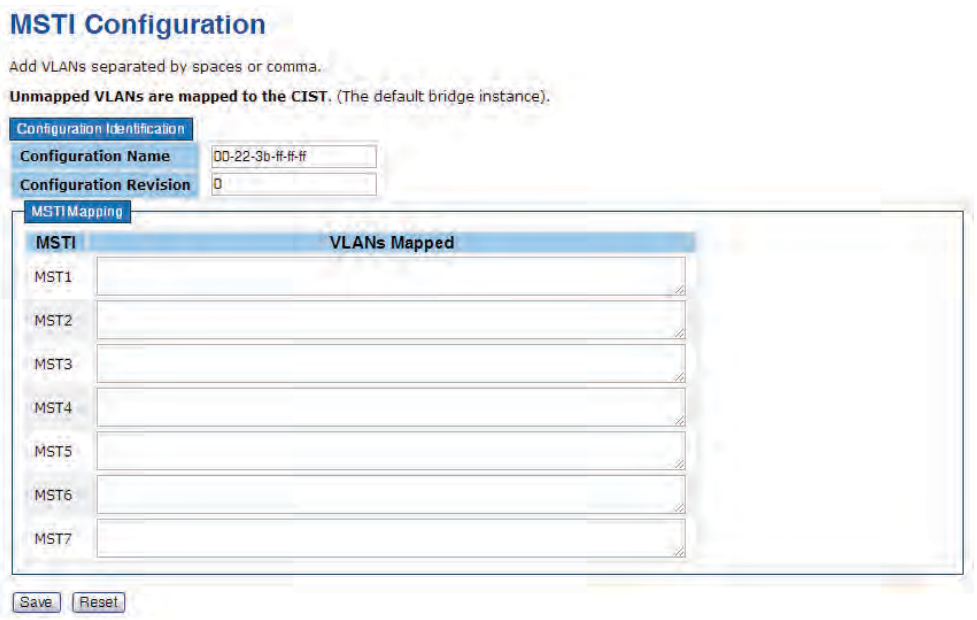
This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.




| Label | Description |
|---|---|
| Protocol Version | The STP protocol version setting. Valid values are STP, RSTP and MSTP. |
| Forward Delay | The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds. |
| Max Age | The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2. |
| Maximum Hop Count | This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2. |
| Transmit Hold Count | The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

## MSTI Mapping

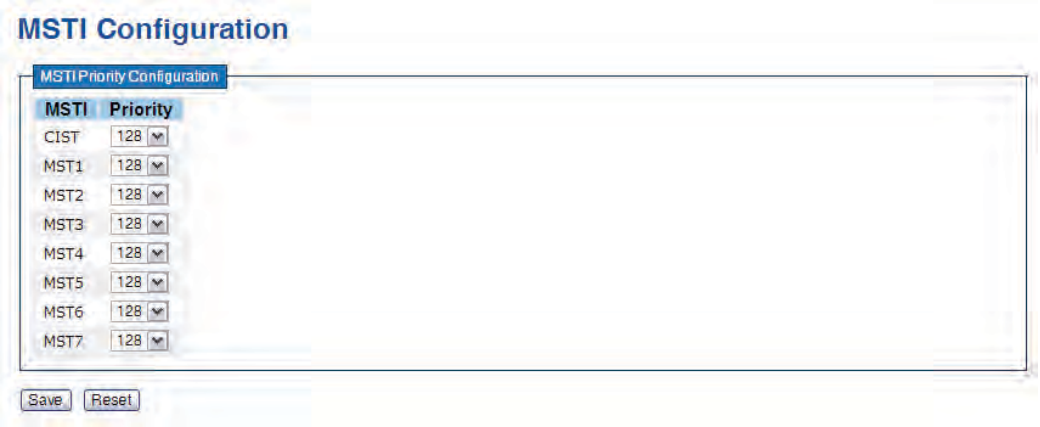
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.




| Label | Description |
|---|---|
| Configuration Name | The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters. |
| Configuration Revision | The revision of the MSTI configuration named above. This must be an integer between 0 and 65535. |
| MSTI | The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. |
| VLANS Mapped | The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (i.e. not having any VLANs mapped to it.) |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

## MSTI Priorities

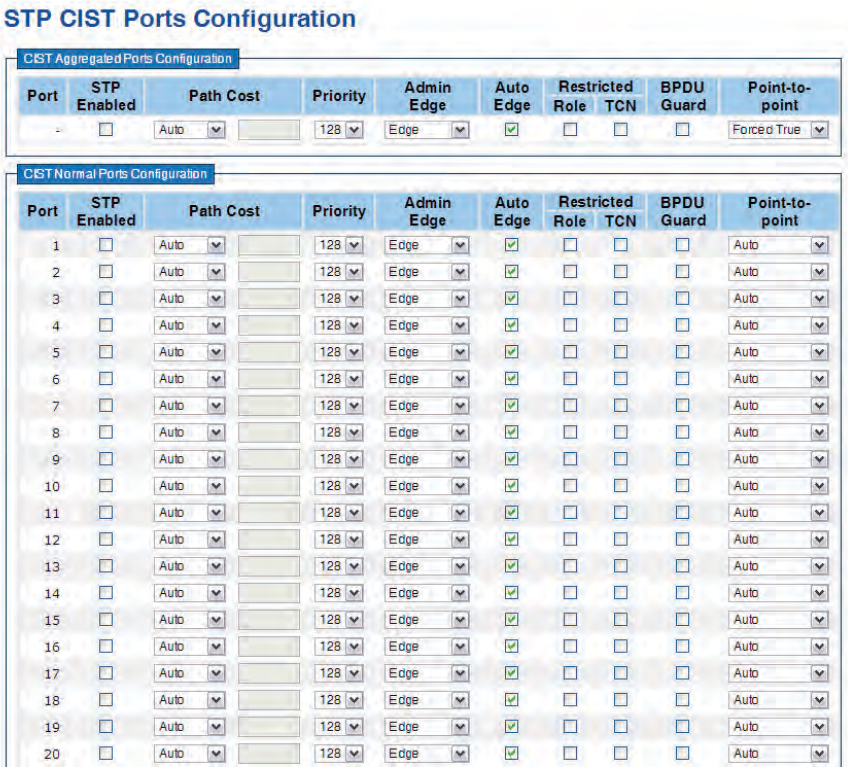
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.




| Label | Description |
|---|---|
| MSTI | The bridge instance. The CIST is the default instance, which is always active. |
| Priority | Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

## CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports. The aggregation settings are stack global.

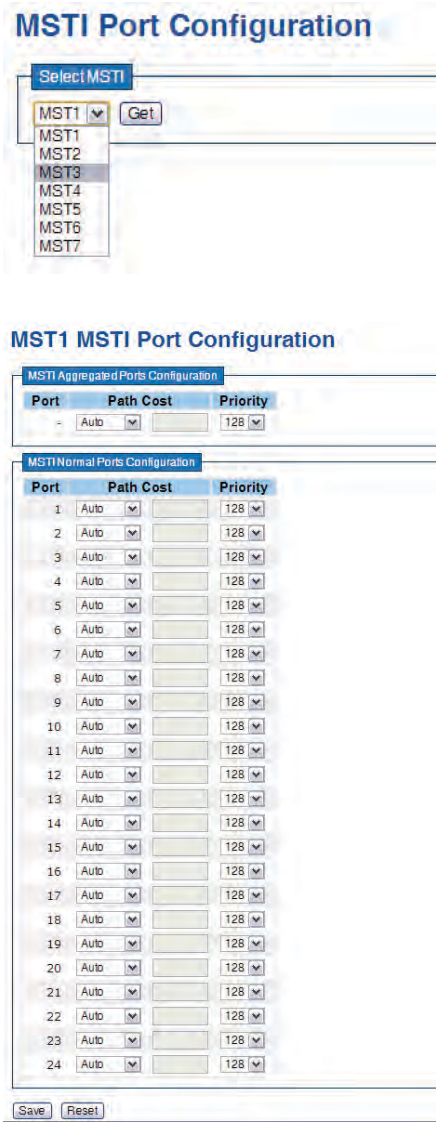


| Label | Description |
|---|---|
| Port | The switch port number of the logical STP port. |
| STP Enabled | Controls whether STP is enabled on this switch port. |
| Path Cost | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| Priority | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |
| OpenEdge (state flag) | Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having OpenEdge true) than for other ports. |
| AdminEdge | Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized). |
| AutoEdge | Controls whether the bridge should enable automatic edge detection on the bridge port. This allows OpenEdge to be derived from whether BPDU's are received on the port or not. |
| Restricted Role | If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard. |
| Restricted TCN | If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently. |
| Point2Point | Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

## MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are stack global.

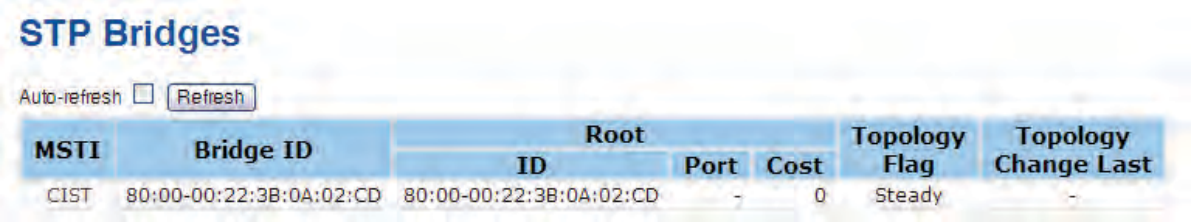


| Label | Description |
|---|---|
| Port | The switch port number of the corresponding STP CIST (and MSTI) port. |
| Path Cost | Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000. |
| Priority | Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). |
| Save | Select to save changes. |
| Reset | Select to undo any changes made locally and revert to previously saved values. |

## STP Bridges

This page provides a status overview for all STP bridge instances.

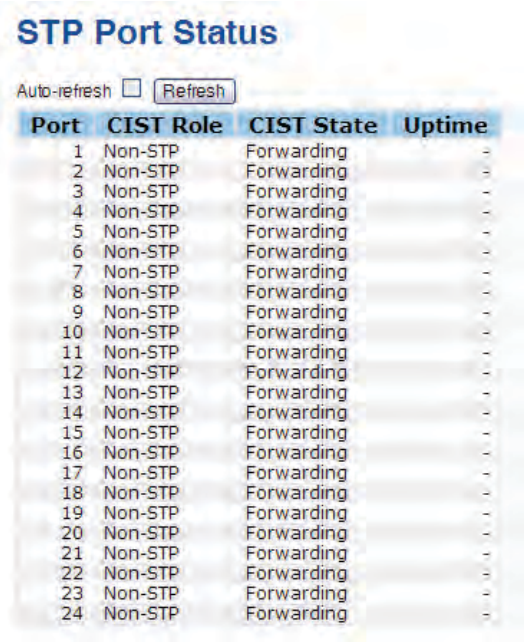
The displayed table contains a row for each STP bridge instance, where the columns display the following information:




| Label | Description |
|---|---|
| MSTI | The Bridge Instance. This is also a link to the STP Detailed Bridge Status. |
| Bridge ID | The Bridge ID of this Bridge instance. |
| Root ID | The Bridge ID of the currently elected root bridge. |
| Root Port | The switch port currently assigned the root port role. |
| Root Cost | Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| Topology Flag | The current state of the Topology Change Flag for this Bridge instance. |
| Topology Change Last | The time since last Topology Change occurred. |
| Refresh | Select to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

## STP Port Status

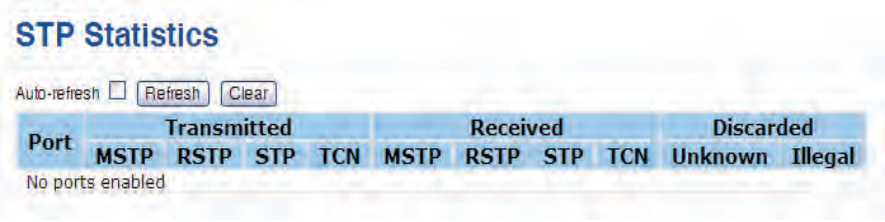
This page displays the STP CIST port status for port physical ports in the currently selected switch.




| Label | Description |
|---|---|
| Port | The switch port number of the logical STP port. |
| CIST Role | The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort. |
| State | The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding. |
| Uptime | The time since the bridge port was last initialized. |
| Refresh | Select to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

## STP Statistics

This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.

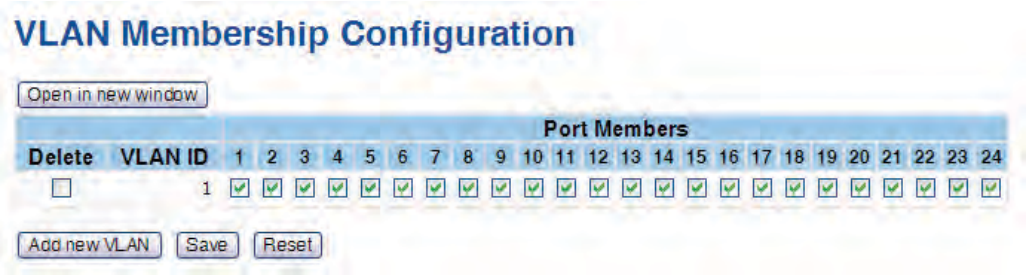



| Label | Description |
|---|---|
| Port | The switch port number of the logical RSTP port. |
| RSTP | The number of RSTP Configuration BPDUs received/transmitted on the port. |
| STP | The number of legacy STP Configuration BPDUs received/transmitted on the port. |
| TCN | The number of (legacy) Topology Change Notification BPDUs received/transmitted on the port. |
| Discarded Unknown | The number of unknown Spanning Tree BPDUs received (and discarded) on the port. |
| Discarded Illegal | The number of illegal Spanning Tree BPDUs received (and discarded) on the port. |
| Refresh | Select to refresh the page immediately. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

## VLAN

### VLAN Membership Configuration

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

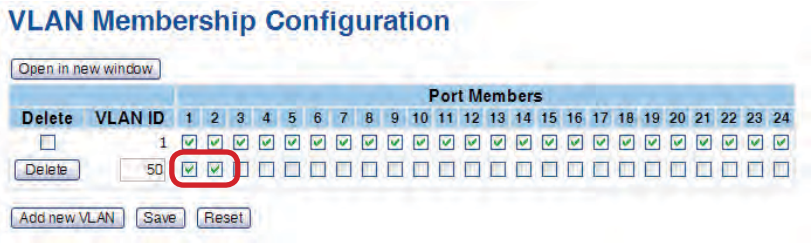

VLAN Membership Configuration
Open in new window
Port Members
Delete
VLAN ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1
Add new VLAN
Save
Reset

| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| VLAN ID | The VLAN ID for the entry. |
| MAC Address | The MAC address for the entry. |
| Port Members | Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry. |
| Add new VLAN | Select to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.<br>The VLAN is enabled on the selected stack switch unit when you Select on **Save**. The VLAN is thereafter present on the other stack switch units, but with no port members.<br>A VLAN without any port members on any stack unit will be deleted when you select **Save**.<br>The **Reset** button can be used to undo the addition of new VLANs. |

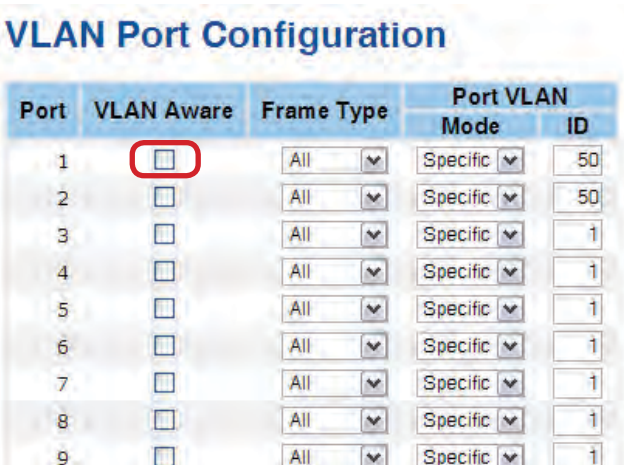
Example:

Portbased VLAN Setting (For ingress port)

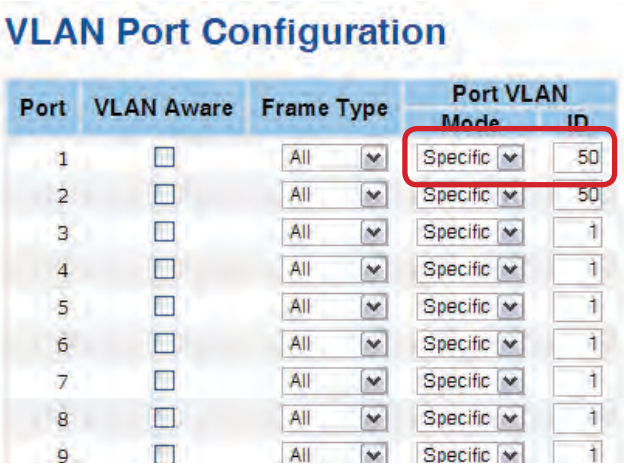
1. VLAN Membership Configuration setting port 1 & VID=50




2. VLAN Port 1 Configurations-->Disable VLAN Aware

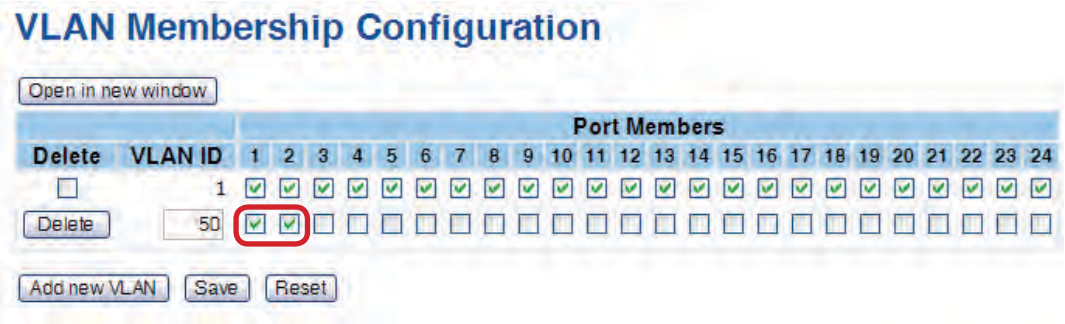



3. VLAN Port 1 Configuration-->Mode=specific,ID=50

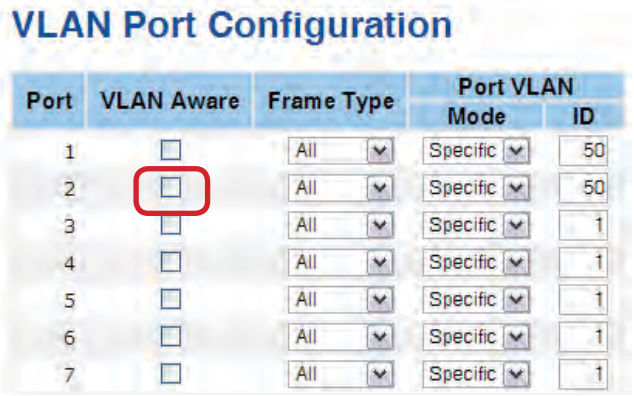


(For egress port)

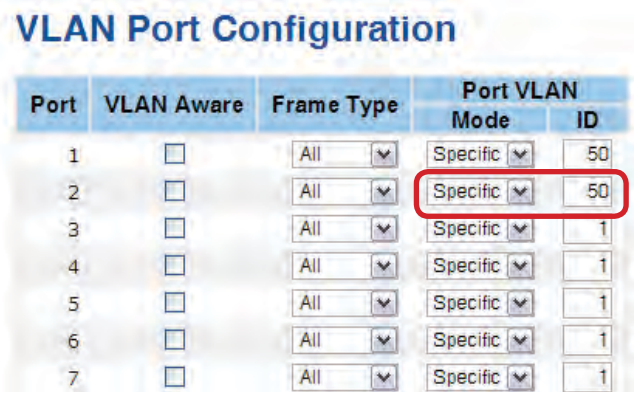
1. VLAN Membership Configuration setting port 2 & VID=50




2. VLAN Port 2 Configuration-->don't care VLAN Aware



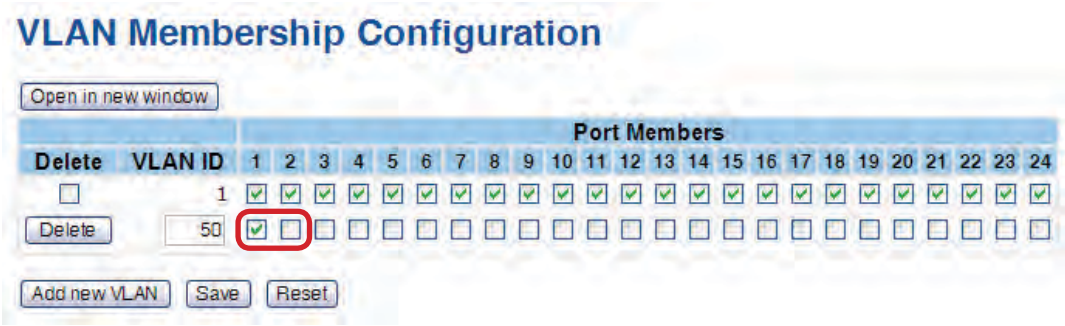

3. VLAN Port 2 Configuration-->Mode=specific, ID=50
   (Any packet can enter egress port )



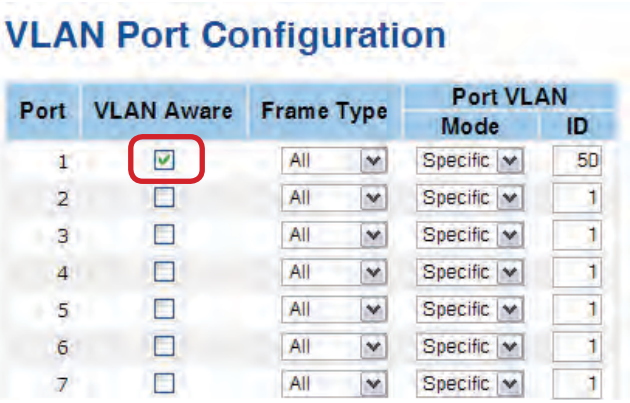
802.1Q Access port Setting

(For ingress port)

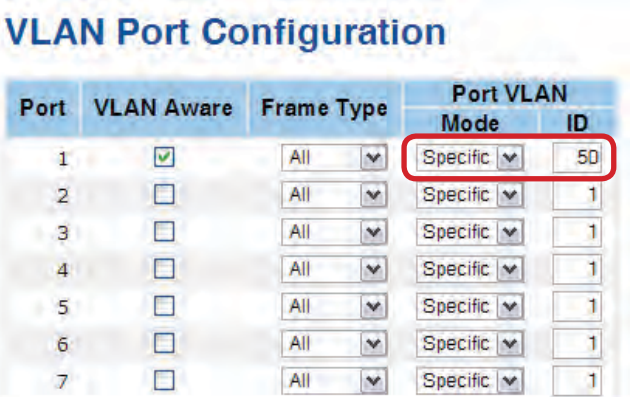
1. VLAN Membership Configuration setting port & VID=50




2. VLAN Port Configurations-->Enable VLAN Aware

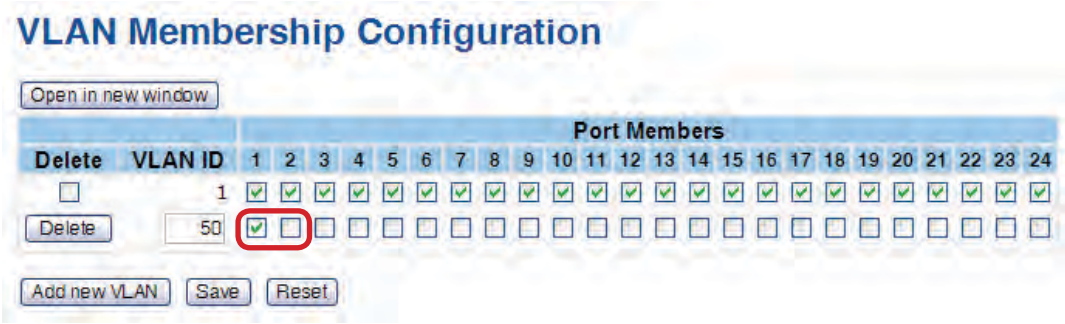



1. VLAN Port Configuration-->Mode=specific,ID=50

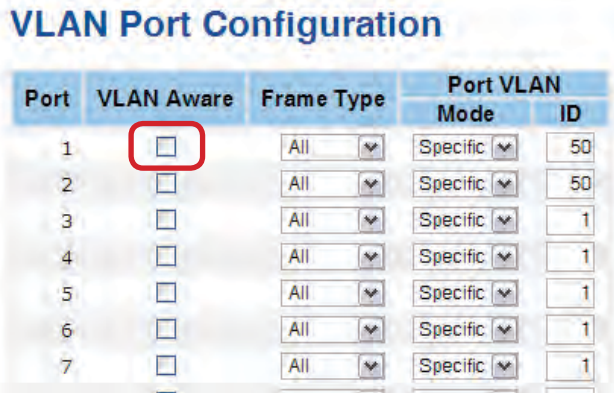


(For egress port)

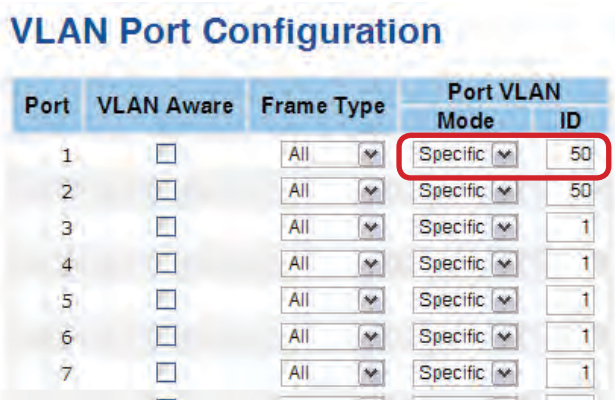
1. VLAN Membership Configuration setting port & VID=50



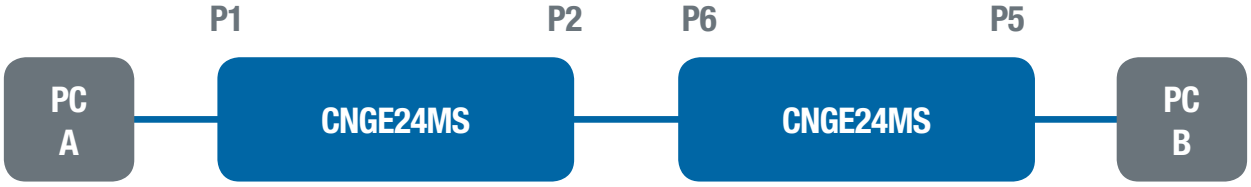

2. VLAN Port Configurations-->Disable VLAN Aware




3. VLAN Port Configuration-->Mode=specific,ID=50
(Untagged & tag=50 packet can enter egress port )

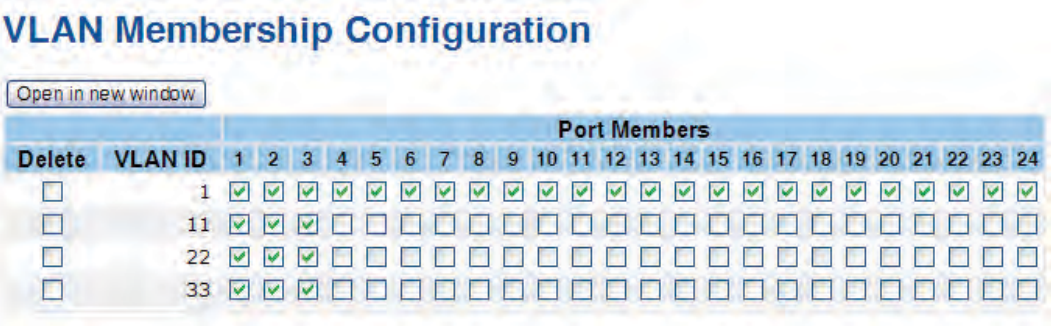


802.1Q Trunk port setting (multi-tag)

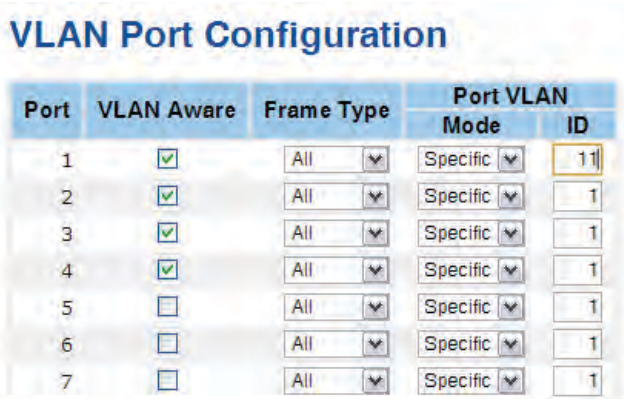



(For ingress port)

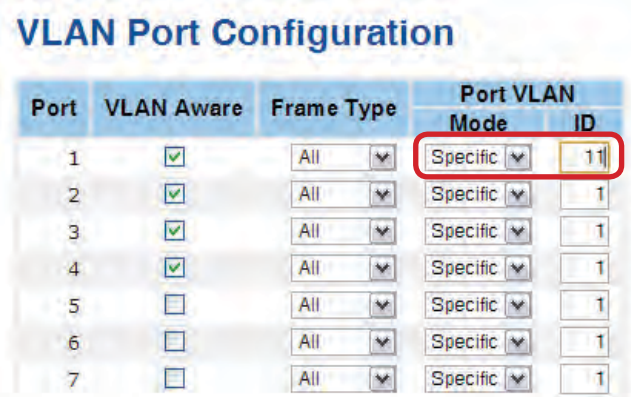
1. VLAN Membership Configuration setting port & VID=11,22,33


VLAN Membership Configuration
Open in new window
Port Members
Delete VLAN ID 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1
11
22
33

2. VLAN Port Configurations-->Enable VLAN Aware

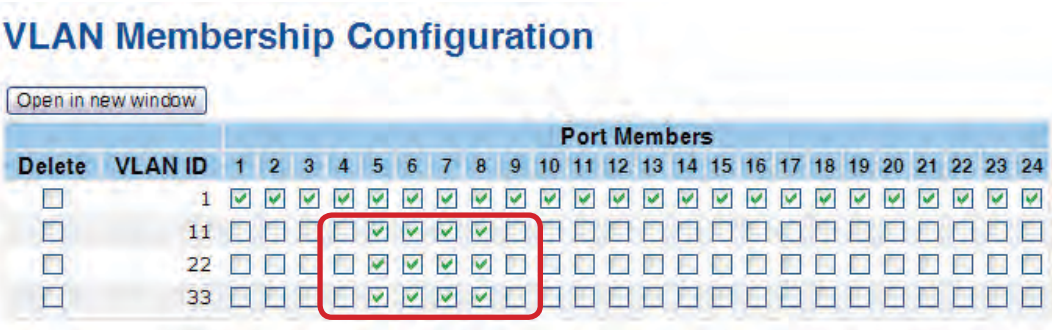

VLAN Port Configuration
Port VLAN Aware Frame Type Port VLAN Mode ID
1 All Specific 11
2 All Specific 1
3 All Specific 1
4 All Specific 1
5 All Specific 1
6 All Specific 1
7 All Specific 1

3. VLAN Port Configuration-->Mode=specific,ID=11
(when entering packet is untagged frame, added tag = 11
When entering the tagged frame, only VID = 11,22,33 three kinds of packets can pass)

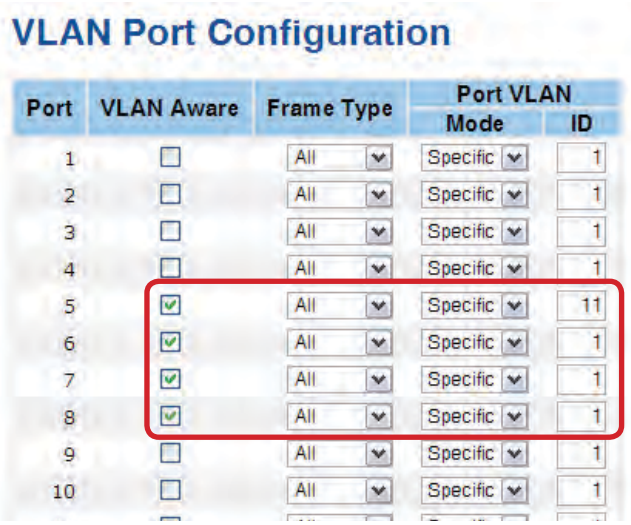



(For egress port)

1. VLAN Membership Configuration setting port, VID=11,22,33


VLAN Membership Configuration
Open in new window
Port Members
Delete
VLAN ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1
11
22
33

2. VLAN Port Configurations-->Enable VLAN Aware

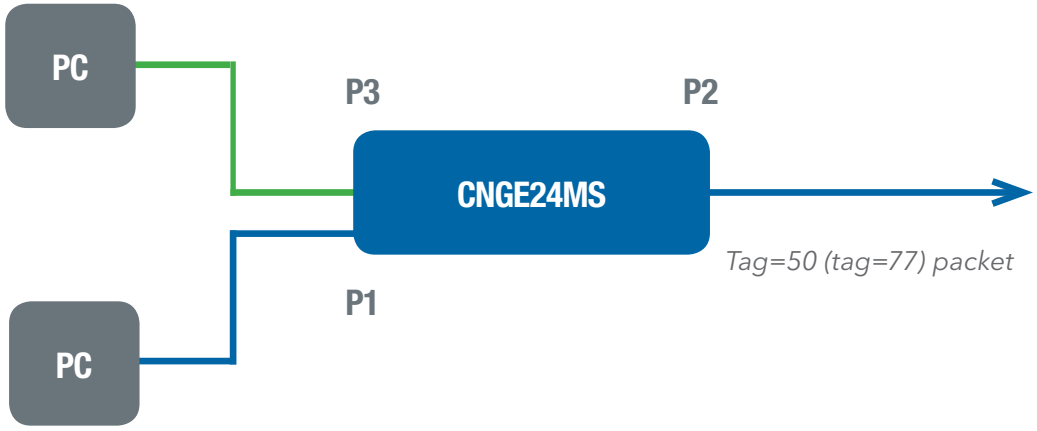



3. VLAN Port Configuration-->Mode=none
   (Egress port can receive tag=11,22,33 packet
   In addition, only tag=11 packet can enter egress port)

## VLAN Port Configuration

| Port | VLAN Aware | Frame Type | Port VLAN Mode | Port VLAN ID |
|---|---|---|---|---|
| 1 | ☐ | All | Specific | 1 |
| 2 | ☐ | All | Specific | 1 |
| 3 | ☐ | All | Specific | 1 |
| 4 | ☐ | All | Specific | 1 |
| 5 | ☑ | All | Specific | 11 |
| 6 | ☑ | All | Specific | 1 |
| 7 | ☑ | All | Specific | 1 |
| 8 | ☑ | All | Specific | 1 |
| 9 | ☐ | All | Specific | 1 |
| 10 | ☐ | All | Specific | 1 |

QinQ VLAN Setting




*ingress Port 1---------->egress Port 2*

(For Ingress port----- Port 1)

1. VLAN Membership Configuration setting port 1, 2 and 3 & VID=50

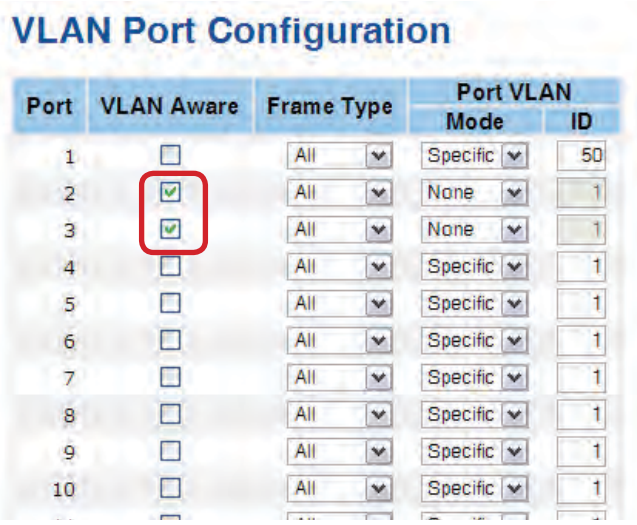
## VLAN Membership Configuration

Open in new window

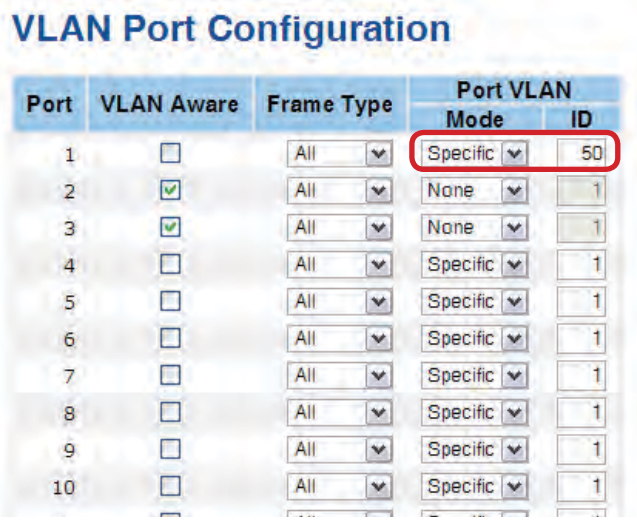
| Delete | VLAN ID | Port Members 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| ☐ | 50 | ☑ | ☑ | ☑ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Add new VLAN | Save | Reset

2. VLAN Port Configuration-->Disable Port 1 VLAN Aware

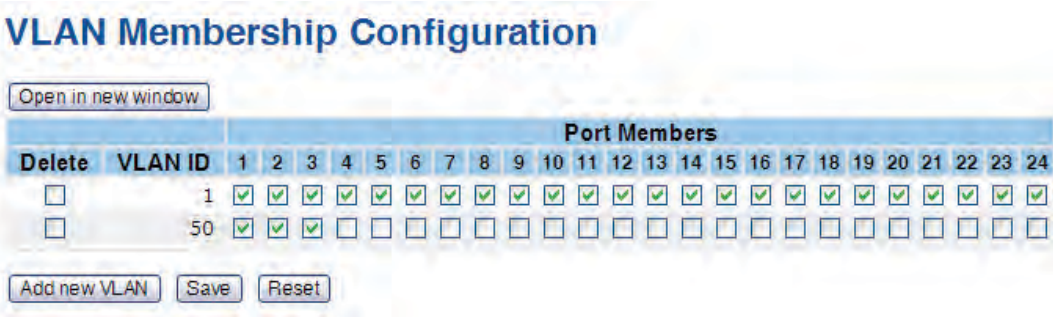



3. VLAN Port Configuration-->Port 1 Mode=specific, ID=50

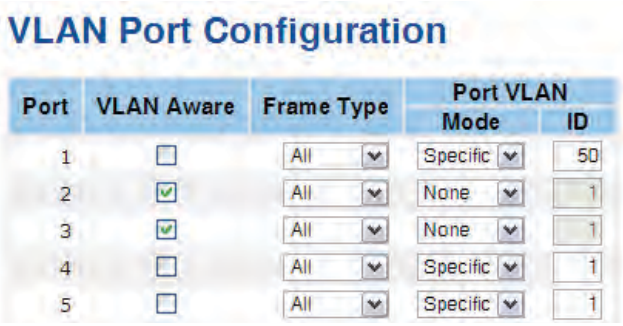


(For egress port ----Port 2)

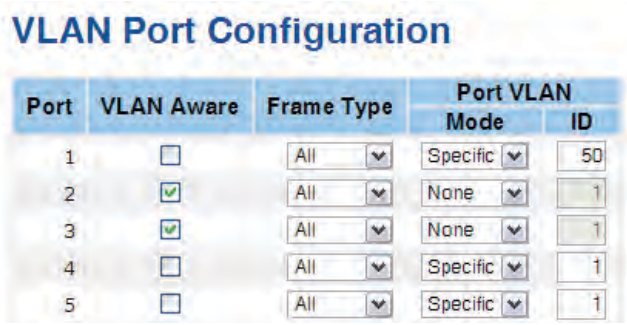
1. VLAN Membership Configuration setting port & VID=50


VLAN Membership Configuration
Open in new window
Port Members
Delete VLAN ID 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1
50
Add new VLAN
Save
Reset

2. VLAN Port Configuration-->Enable Port 2 and 3 VLAN Aware.


VLAN Port Configuration
Port VLAN Aware Frame Type Port VLAN Mode ID
1 All Specific 50
2 All None 1
3 All None 1
4 All Specific 1
5 All Specific 1

3. VLAN Port Configuration-->Mode=none
(only tag=50 packet can enter egress port )


VLAN Port Configuration
Port VLAN Aware Frame Type Port VLAN Mode ID
1 All Specific 50
2 All None 1
3 All None 1
4 All Specific 1
5 All Specific 1

### Private VLAN

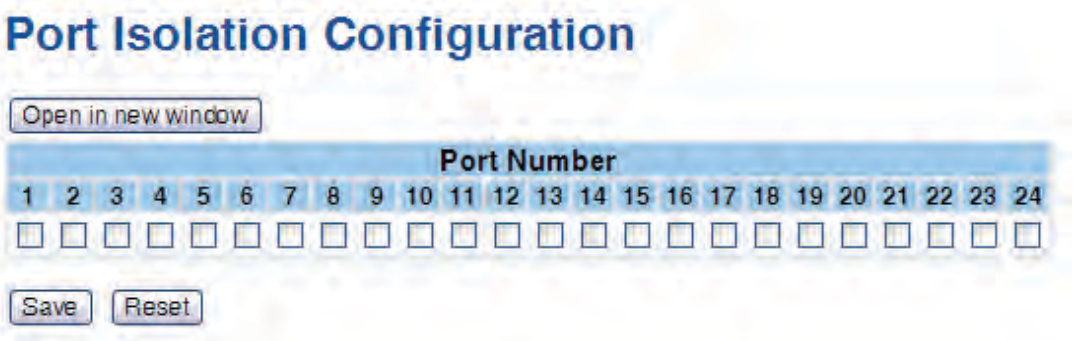
The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Private VLAN Membership Configuration
Open in new window
Port Members
Delete
PVLAN ID
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
1
Add new Private VLAN
Save
Reset

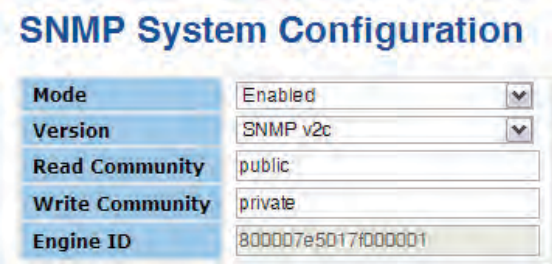
| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Private VLAN ID | Indicates the ID of this particular private VLAN. |
| MAC Address | The MAC address for the entry. |
| Port Members | A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked. |
| Add New Private VLAN | Select **Add New Private VLAN** to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Select **OK** to discard the incorrect entry, or Select **Cancel** to return to the editing and make a correction.<br>The Private VLAN is enabled when you Select **Save**.<br>The **Delete** button can be used to undo the addition of new Private VLANs. |




| Label | Description |
|---|---|
| Port Members | A check box is provided for each port of a private VLAN.<br>When checked, port isolation is enabled for that port.<br>When unchecked, port isolation is disabled for that port.<br>By default, port isolation is disabled for all ports. |

## SNMP

### SNMP-System




| Label | Description |
|---|---|
| Mode | Indicates the SNMP mode operation. Possible modes are:<br>Enabled: Enable SNMP mode operation.<br>Disabled: Disable SNMP mode operation. |
| Version | Indicates the SNMP supported version. Possible versions are:<br>SNMP v1: Set SNMP supported version 1.<br>SNMP v2c: Set SNMP supported version 2c.<br>SNMP v3: Set SNMP supported version 3. |
| Read Community | Indicates the community read access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.<br>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table |
| Write Community | Indicates the community write access string to permit access to SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.<br>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will be associated with SNMPv3 communities table. |
| Engine ID | Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users. |

| Label | Description |
|---|---|
| Trap Mode | Indicates the SNMP trap mode operation. Possible modes are:<br>Enabled: Enable SNMP trap mode operation.<br>Disabled: Disable SNMP trap mode operation. |
| Trap Version | Indicates the SNMP trap supported version. Possible versions are:<br>SNMP v1: Set SNMP trap supported version 1.<br>SNMP v2c: Set SNMP trap supported version 2c.<br>SNMP v3: Set SNMP trap supported version 3. |
| Trap Community | Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. |
| Trap Destination Address | Indicates the SNMP trap destination address.<br>Trap Destination IPv6 Address |
| Trap Destination IPv6 Address | Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80:215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'. |
| Trap Authentication Failure | Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are:<br>Enabled: Enable SNMP trap authentication failure.<br>Disabled: Disable SNMP trap authentication failure. |
| Trap Link-up and Link-down | Indicates the SNMP trap link-up and link-down mode operation. Possible modes are:<br>Enabled: Enable SNMP trap link-up and link-down mode operation.<br>Disabled: Disable SNMP trap link-up and link-down mode operation. |
| Trap Inform Mode | Indicates the SNMP trap inform mode operation. Possible modes are:<br>Enabled: Enable SNMP trap inform mode operation.<br>Disabled: Disable SNMP trap inform mode operation. |

| | |
|---|---|
| Trap Inform Timeout(seconds) | Indicates the SNMP trap-inform timeout. The allowed range is 0 to 2147. |
| Trap Inform Retry Times | Indicates the SNMP trap inform retry times. The allowed range is 0 to 255. |

### SNMP-Communities

Configure SNMPv3 community's table on this page. The entry index key is Community.

| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Community | Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |
| Source IP | Indicates the SNMP access source address. |
| Source Mask | Indicates the SNMP access source address mask. |

### SNMP-Users

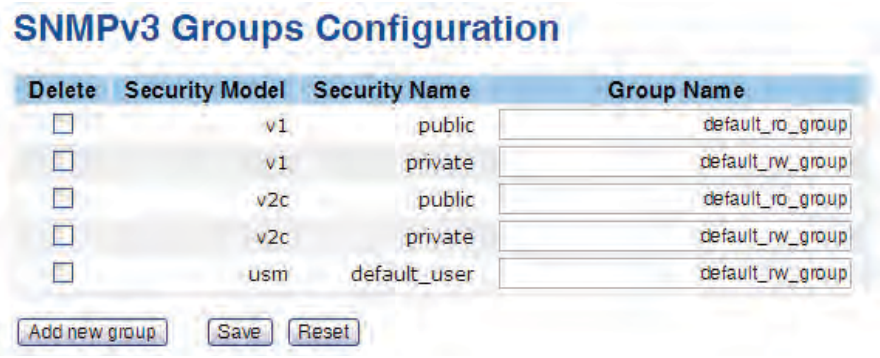
Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.

| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Engine ID | An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user. |
| User Name | A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |
| Security Level | Indicates the security model that this entry should belong to. Possible security models are:<br>NoAuth, NoPriv: No authentication and no privacy.<br>Auth, NoPriv: Authentication and no privacy.<br>Auth, Priv: Authentication and privacy.<br>The value of security level cannot be modified if entry already exists. Ensure that the value is set correctly at the time of entry creation. |
| Authentication Protocol | Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:<br>None: No authentication protocol.<br>MD5: An optional flag to indicate that this user using MD5 authentication protocol.<br>SHA: An optional flag to indicate that this user using SHA authentication protocol.<br>The value of security level cannot be modified if entry already exists. Ensure that the value is set correctly at the time of entry creation |
| Authentication Password | A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32.<br>For SHA authentication protocol, the allowed string length is 8 to 40.<br>The allowed content is the ASCII characters from 33 to 126. |

| | |
|---|---|
| Privacy Protocol | Indicates the privacy protocol that this entry should belong to.<br>Possible privacy protocols are:<br>None: No privacy protocol.<br>DES: An optional flag to indicate that this user is using DES authentication protocol. |
| Privacy Password | A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126. |

### SNMP-Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.




| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Security Model | Indicates the security model that this entry should belong to. Possible security models are:<br>v1: Reserved for SNMPv1.<br>v2c: Reserved for SNMPv2c.<br>usm: User-based Security Model (USM). |
| Security Name | A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |
| Group Name | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |

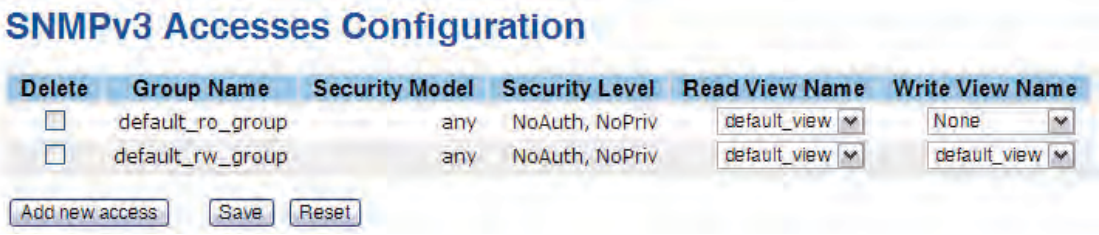
### SNMP-Views

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree.

| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| View Name | A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |
| View Type | Indicates the view type that this entry should belong to. Possible view types are:<br>included: An optional flag to indicate that this view subtree should be included.<br>excluded: An optional flag to indicate that this view subtree should be excluded.<br>Generally, if an entry's view type is 'excluded,' there should exist another entry with the view type 'included' whose OID subtree oversteps the 'excluded' view entry. |
| OID Subtree | The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*). |

### SNMP-Accesses

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.



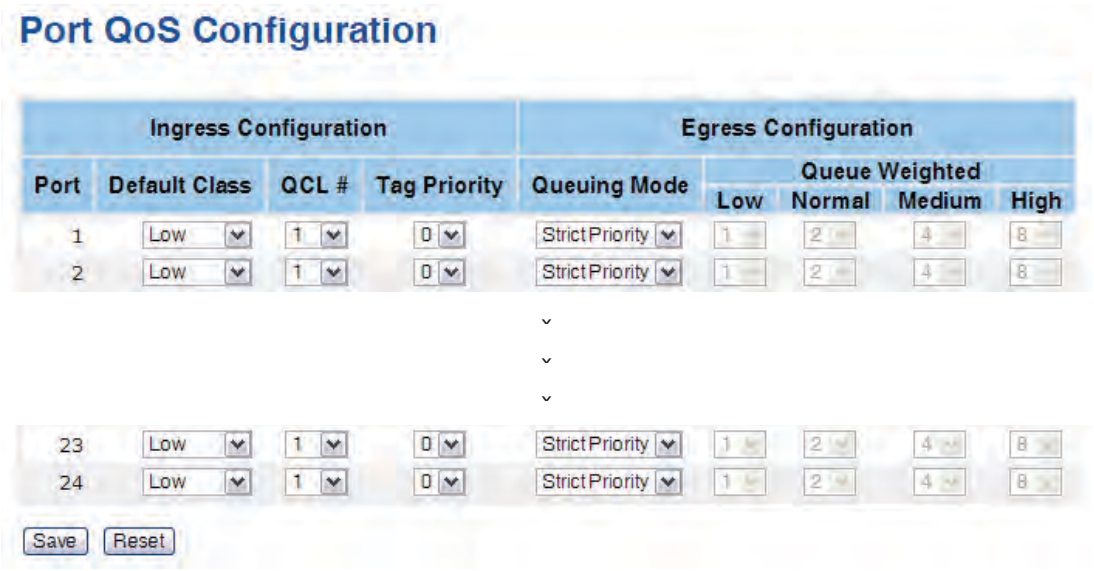

| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| Group Name | A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |
| Security Model | Indicates the security model that this entry should belong to. Possible security models are:<br>any: Accepted any security model (v1\|v2c\|usm).<br>v1: Reserved for SNMPv1.<br>v2c: Reserved for SNMPv2c.<br>usm: User-based Security Model (USM). |
| Security Level | Indicates the security model that this entry should belong to. Possible security models are:<br>NoAuth, NoPriv: No authentication and no privacy.<br>Auth, NoPriv: Authentication and no privacy.<br>Auth, Priv: Authentication and privacy. |
| Read View Name | The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |
| Write View Name | The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. |

## Traffic Prioritization

### Port Configuration

This page allows you to configure QoS settings for each port. Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High. The classification is controlled by a QCL that is assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs. Each QCE can be used to classify certain frames to a specific QoS class. This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS class for the port.




*Port QoS Configuration*

| Label | Description |
|---|---|
| Port | A check box is provided for each port of a private VLAN.<br>When checked, port isolation is enabled for that port.<br>When unchecked, port isolation is disabled for that port.<br>By default, port isolation is disabled for all ports. |
| Default Class | Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL. |
| QCL# | Select which QCL to use for the port. |
| Tag Priority | Select the default tag priority for this port when adding a Tag to the untagged frames. |
| Queuing Mode | Select which Queuing mode for this port. |
| Queue Weighted | Setting Queue weighted (Low=Normal, Medium=High) if the "Queuing Mode" is "Weighted". |

### QoS Control List

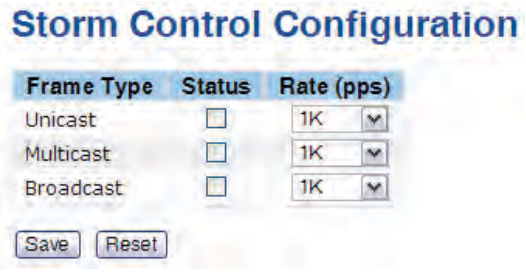
This page lists the QCEs for a given QCL. Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High. The classification is controlled by a QoS assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs. Each QCE can be used to classify certain frames to a specific QoS class. This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS Class for the port.

| Label | Description |
|---|---|
| QCL# | Select a QCL to display a table that lists all the QCEs for that particular QCL. |
| QCE Type | Specifies which frame field the QCE processes to determine the QoS class of the frame. The following QCE types are supported:<br>Ethernet Type: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header.<br>VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged.<br>TCP/UDP Port: IPv4 TCP/UDP source/destination port.<br>DSCP: IPv4 and IPv6 DSCP.<br>ToS: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field).<br>Tag Priority: User Priority. Only applicable if the frame is VLAN tagged or priority tagged. |
| Type Value | Indicates the value according to its QCE type.<br>Ethernet Type: The field shows the Ethernet Type value.<br>VLAN ID: The field shows the VLAN ID.<br>TCP/UDP Port: The field shows the TCP/UDP port range.<br>DSCP: The field shows the IPv4/IPv6 DSCP value. |
| Traffic Class | The QoS class associated with the QCE. |
| Modification Buttons | You can modify each QCE in the table using the following buttons:<br>+ : Inserts a new QCE before the current row.<br>e : Edits the QCE.<br>/\| : Moves the QCE up the list.<br>\|/ : Moves the QCE down the list.<br>× : Deletes the QCE.<br>+ : The lowest plus sign adds a new entry at the bottom of the list of QCL. |

### Storm Control

Storm control for the switch is configured on this page.




There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

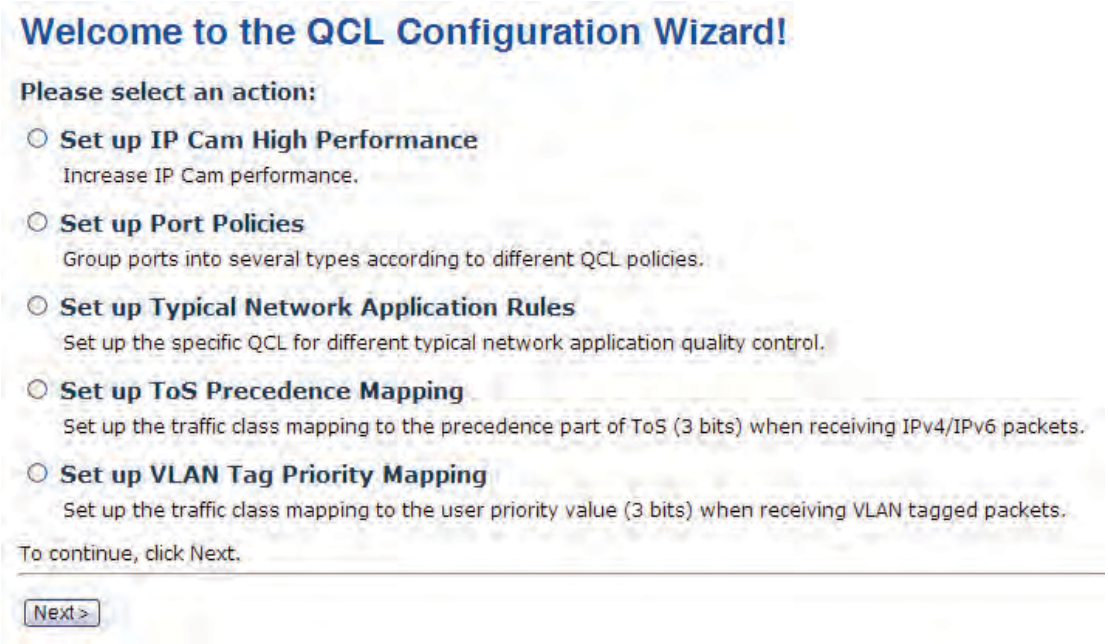
The rate is $2^n$, where $n$ is equal to or less than 15, or "No Limit." The unit of the rate can be either PPS (packets per second) or KPPS (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

(Note: Frames, which are sent to the CPU of the switch are always limited to approximately 4 KPPS. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.)

| Label | Description |
|---|---|
| Frame Type | The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast. |
| Status | Enable or disable the storm control status for the given frame type. |
| Rate | The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.<br>The 1 kpps is actually 1002.1 pps. |

### Wizard

This handy wizard helps you set up a QCL quickly.

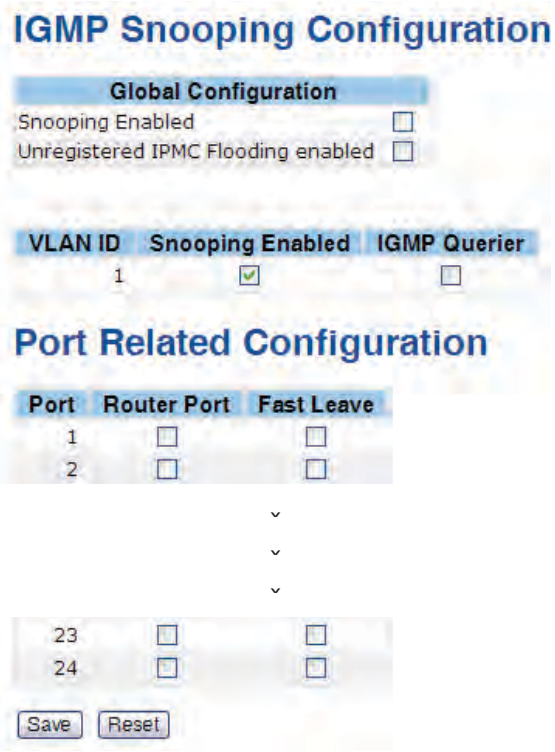

Welcome to the QCL Configuration Wizard!
Please select an action:
Set up IP Cam High Performance
Increase IP Cam performance.
Set up Port Policies
Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules
Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.
To continue, click Next.
Next >

| Label | Description |
|---|---|
| Set up Port Policies | Group ports into several types according to different QCL policies. |
| Set up Typical Network Application Rules | Set up the specific QCL for different typical network application quality control. |
| Set up ToS Precedence Mapping | Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets. |
| Set up VLAN Tag Priority Mapping | Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets. |

## Multicast

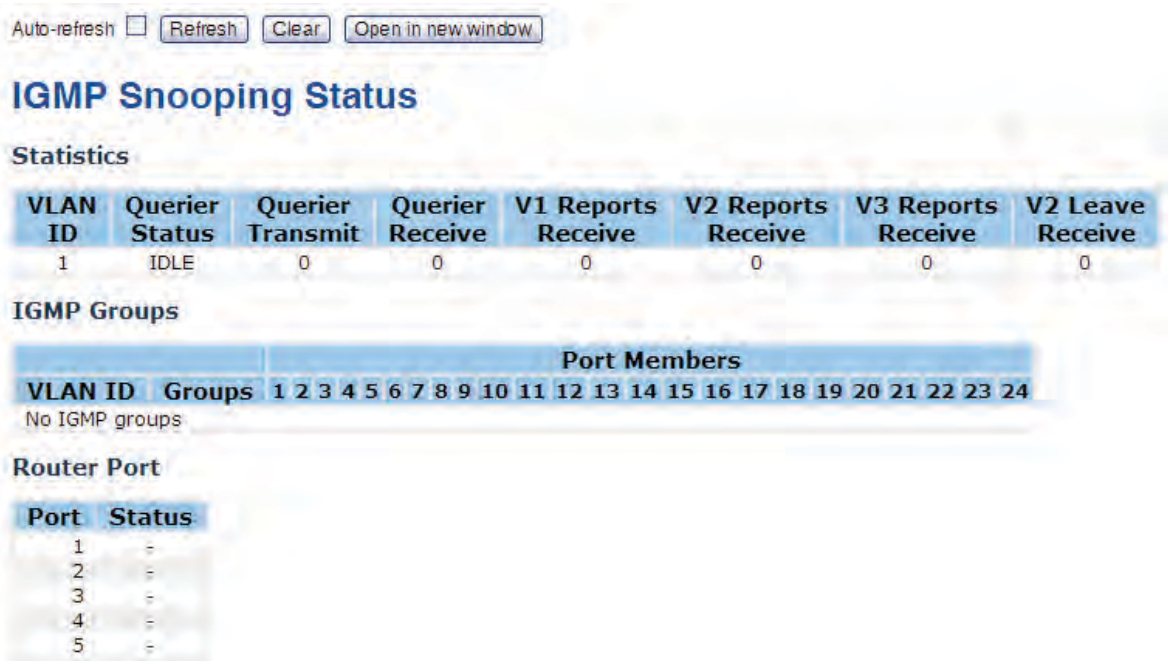
### IGMP Snooping

This page provides IGMP Snooping related configuration.




| Label | Description |
|---|---|
| Snooping Enabled | Enable the Global IGMP Snooping. |
| Unregistered IPMC Flooding enabled | Enable unregistered IPMC traffic flooding. |
| VLAN ID | The VLAN ID of the entry. |
| IGMP Snooping Enabled | Enable the per-VLAN IGMP Snooping. |
| IGMP Querier | Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices. |
| Router Port | Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.<br>If an aggregation member port is selected as a router port, the whole aggregation will act as a router port. |
| Fast Leave | Enable the fast leave on the port. |

## IGMP Snooping Status

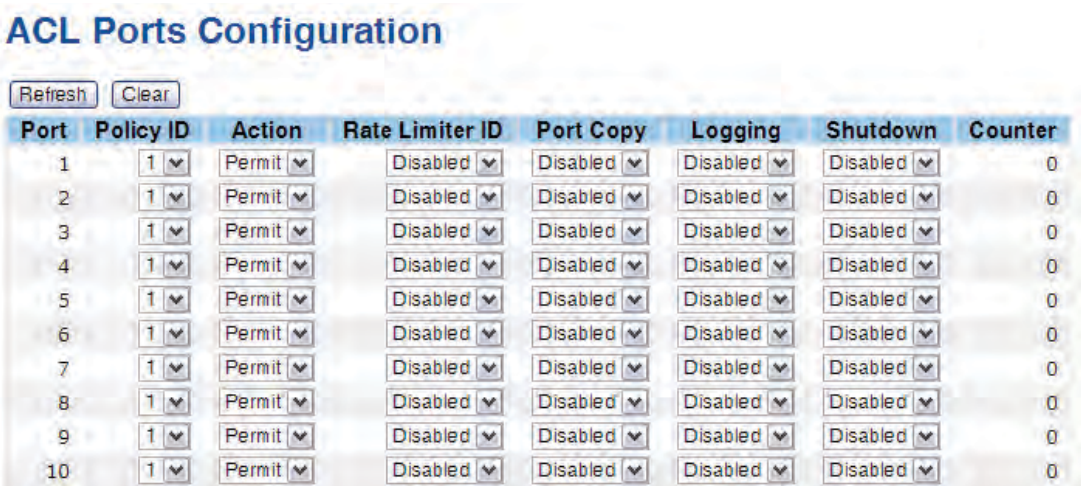



| Label | Description |
|---|---|
| VLAN ID | The VLAN ID of the entry. |
| Groups | The present IGMP groups. Maximum of 128 groups for each VLAN. |
| Port Members | The ports that are members of the entry. |
| Querier Status | Show the Querier status is “ACTIVE” or “IDLE” |
| Querier Receive | The number of Transmitted Querier |
| V1 Reports Receive | The number of Received V1 Reports |
| V2 Reports Receive | The number of Received V2 Reports |
| V3 Reports Receive | The number of Received V3 Reports |
| V2 Leave Receive | The number of Received V2 Leave |
| Refresh | Select to refresh the page immediately |
| Clear | Clears all Statistics counters |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |

## Security

### ACL

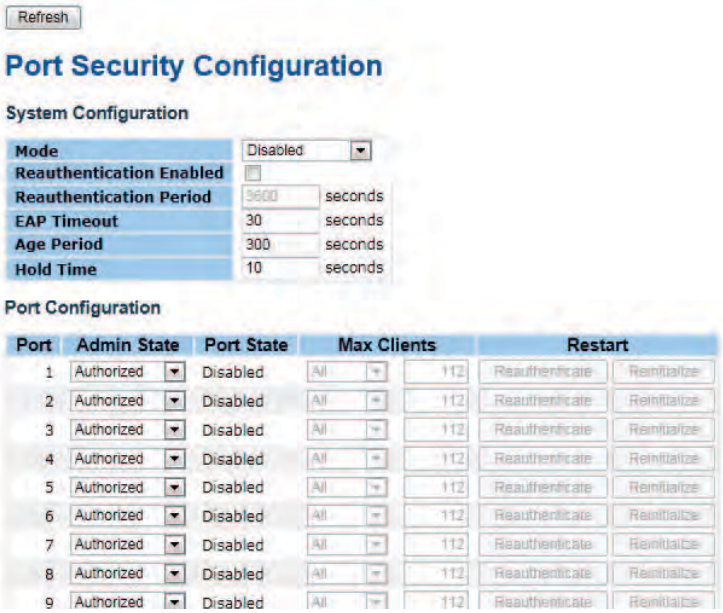
Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.


ACL Ports Configuration
Refresh
Clear
Port
Policy ID
Action
Rate Limiter ID
Port Copy
Logging
Shutdown
Counter
1 1 Permit Disabled Disabled Disabled Disabled 0
2 1 Permit Disabled Disabled Disabled Disabled 0
3 1 Permit Disabled Disabled Disabled Disabled 0
4 1 Permit Disabled Disabled Disabled Disabled 0
5 1 Permit Disabled Disabled Disabled Disabled 0
6 1 Permit Disabled Disabled Disabled Disabled 0
7 1 Permit Disabled Disabled Disabled Disabled 0
8 1 Permit Disabled Disabled Disabled Disabled 0
9 1 Permit Disabled Disabled Disabled Disabled 0
10 1 Permit Disabled Disabled Disabled Disabled 0

| Label | Description |
|---|---|
| Port | The logical port for the settings contained in the same row. |
| Policy ID | Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1. |
| Action | Select whether forwarding is permitted (“Permit”) or denied (“Deny”). The default value is “Permit”. |
| Rate Limiter ID | Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is “Disabled”. |
| Port Copy | Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is “Disabled”. |
| Logging | Specify the logging operation of this port. The allowed values are:<br>Enabled: Frames received on the port are stored in the System Log.<br>Disabled: Frames received on the port are not logged.<br>The default value is “Disabled”. Please note that the System Log memory size and logging rate is limited. |
| Shutdown | Specify the port shut down operation of this port. The allowed values are:<br>Enabled: If a frame is received on the port, the port will be disabled.<br>Disabled: Port shut down is disabled.<br>The default value is “Disabled”. |
| Counter | Counts the number of frames that match this ACE. |

### IEEE 802.1x

This page allows you to configure how an administrator is authenticated when he logs into the switch-stack via TELNET, SSH or the web pages.




*Client Configuration*

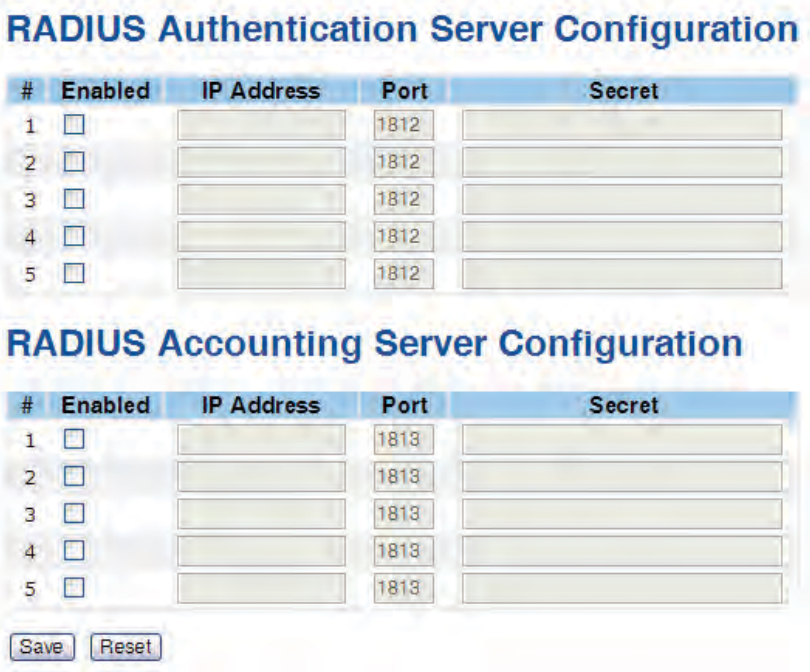
The table has one row for each Client and a number of columns, which are:

| Label | Description |
|---|---|
| Mode | Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames. |
| Reauthentication Enabled | If checked, clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port.<br>For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below). |
| Reauthentication Period | Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds. |
| EAP Timeout | Determines the time the switch shall wait for the supplicant response before retransmitting a packet. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports. |

| | |
|---|---|
| Age Period | This setting applies to ports running MAC-based authentication, only. Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that runs MAC-based authentication, and suppose the client gets successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Reauthentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging of authenticated clients. The Age Period, which can be set to a number between 10 and 1000000 seconds, works like this: A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 for him to stay authenticated. |
| Hold Time | This setting applies to ports running MAC-based authentication, only. If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout specified on the Authentication configuration page), the client is put on hold in the Unauthorized state. In this state, frames from the client will not cause the switch to attempt to reauthenticate the client. The Hold Time, which can be set to a number between 10 and 1000000 seconds, determines the time after an EAP Failure indication or RADIUS timeout that a client is not allowed access. |
| Port | The port number for which the configuration below applies. |
| Admin State | • Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled): Auto: Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.<br>• Authorized: Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up.<br>• Unauthorized: Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up.<br>• MAC-Based: Enables MAC-based authentication on the port. The switch doesn't transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind. |

| | |
|---|---|
| Port State | The current state of the port. It can undertake one of the following values:<br>• Disabled: 802.1X and MAC-based authentication is globally disabled.<br>• Link Down: 802.1X or MAC-based authentication is enabled, but there is no link on the port.<br>• Authorized: The port is authorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto" and the supplicant is authenticated or the Admin State is "Authorized".<br>• Unauthorized: The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto", but the supplicant is not (yet) authenticated or the Admin State is "Unauthorized".<br>• X Auth/Y Unauth: X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based". |
| Max Clients | This setting applies to ports running MAC-based authentication, only. The maximum number of clients allowed on a given port can be configured through the list-box and edit-control for this setting. Choosing the value "All" from the list-box allows the port to consume up to 48 client state-machines. Choosing the value "Specific" from the list-box opens up for entering a specific number of maximum clients on the port (1 to 48).<br>The switch is "born" with a pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (both authorized and unauthorized clients count), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines. |
| Restart | Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is "Auto" or "MAC-Based". Clicking these buttons will not cause settings changed on the page to take effect.<br>• Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.<br>• The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized.<br>• Reinitialize: Forces a reinitialization of the port/clients and thereby a reauthentication immediately. The port/clients will transfer to the unauthorized state while the reauthentication is ongoing. |

## RADIUS Authentication Server Configuration



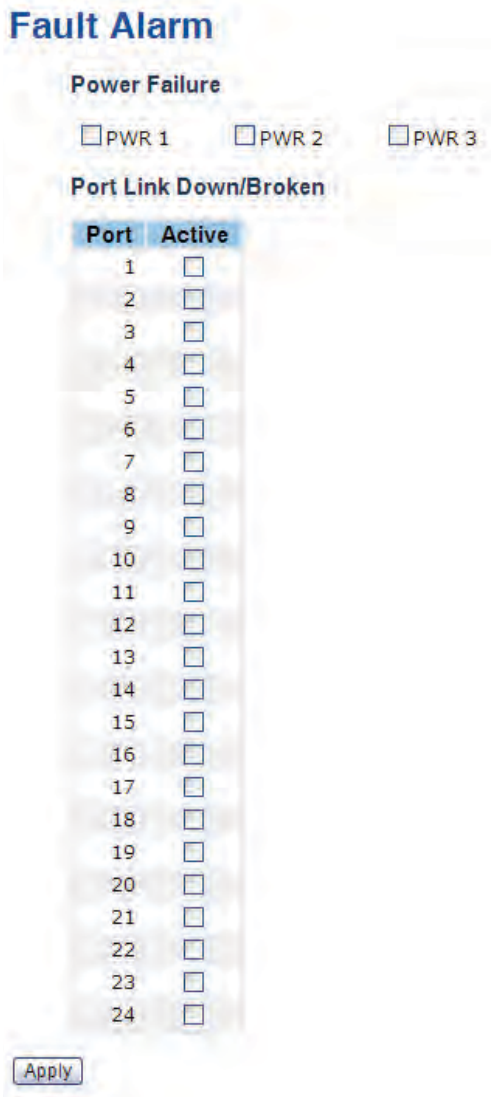

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

| Label | Description |
|---|---|
| # | The RADIUS Authentication Server number for which the configuration below applies. |
| Enabled | Enable the RADIUS Authentication Server by checking this box. |
| IP Address | Enable fallback to local authentication by checking this box.<br>If none of the configured authentication servers are alive, the local user database is used for authentication.<br>This is only possible if the Authentication Method is set to something else than 'none' or 'local'. |
| Port | The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server. |
| Secret | The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch-stack. |

### Warning

### Fault Alarm

When any selected fault event is happening, the Fault LED in switch panel will light up and the relay will signal at the same time.

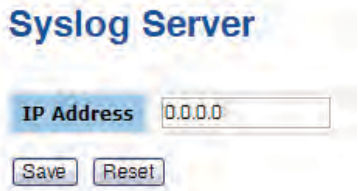



The following table describes the labels in this screen.

| Label | Description |
|---|---|
| Power Failure | Mark the blank of PWR 1 , PWR 2 or PWR 3 to monitor. |
| Port Link Down/ Broken | Mark the blank of port 1 to port 24 to monitor. |
| Apply | Select **Apply** to set the configurations. |

### System Warning

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol



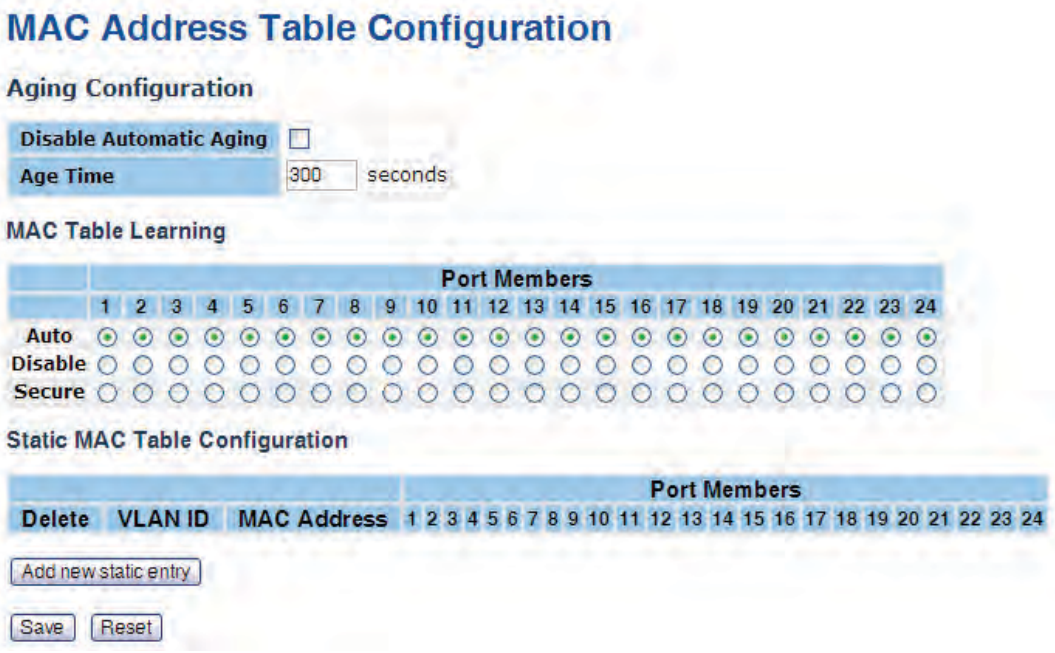

The following table describes the labels in this screen.

| Label | Description |
|---|---|
| IP Address | The remote SYSLOG Server IP address. |
| Save | Select to save the configurations. |
| Reset | Select to clear any unsaved changes and reset configuration. |

### Monitor and Diag

### MAC Table

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

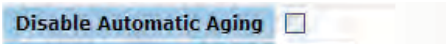

MAC Address Table Configuration
Aging Configuration
Disable Automatic Aging
Age Time
300
seconds
MAC Table Learning
Port Members
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Auto
Disable
Secure
Static MAC Table Configuration
Port Members
Delete
VLAN ID
MAC Address
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Add new static entry
Save
Reset

## Aging Configuration

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds. The allowed range is 10 to 1000000 seconds.

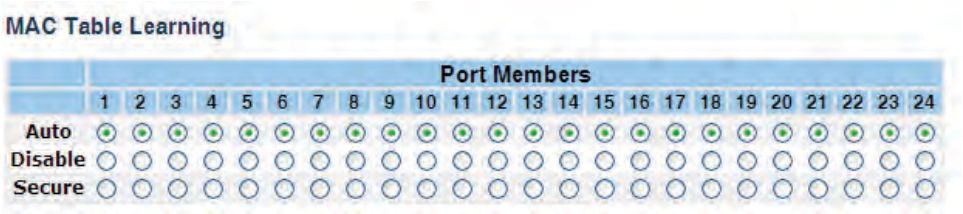
Disable the automatic aging of dynamic entries by checking:




## MAC Table Learning

If the learning mode for a given port is grayed out, another module is in control of the mode and the user cannot change it. An example of such a module is the MAC-Based Authentication under 802.1X.

Each port can perform learning based upon the following settings:




| Label | Description |
|---|---|
| Auto | Learning is done automatically as soon as a frame with unknown SMAC is received. |
| Disable | No learning is done. |
| Secure | Only static MAC entries are learned, all other frames are dropped. Note: Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface. |

## Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries.

The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

| Label | Description |
|---|---|
| Delete | Check to delete the entry. It will be deleted during the next save. |
| VLAN ID | The VLAN ID for the entry. |
| MAC Address | The MAC address for the entry. |
| Port Members | Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry. |
| Adding a New Static Entry | Select **Add new static entry** to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Select **Save**. |

### Mirroring

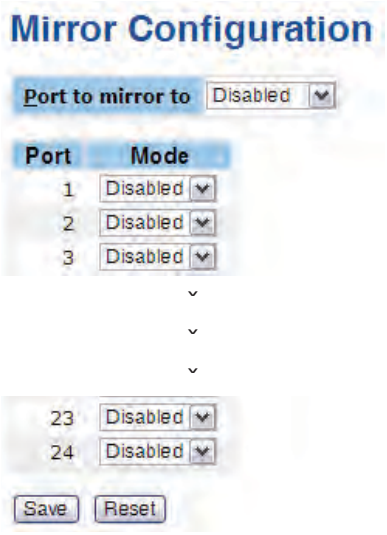
Configure Port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source Mirroring).

All frames transmitted on a given port (also known as egress or destination Mirroring).

Port to mirror also known as the mirror port. Frames from ports that have either source (RX) or destination (TX) Mirroring enabled are mirrored to this port. Disabled disables Mirroring.




| Label | Description |
|---|---|
| Port | The logical port for the settings contained in the same row. |
| Mode | Select mirror mode.<br>Rx only: Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored.<br>TX only: Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored.<br>Disabled: Neither frames transmitted nor frames received are mirrored.<br>Enabled: Frames received and frames transmitted are mirrored to the mirror port.<br>Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror TX frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only. |

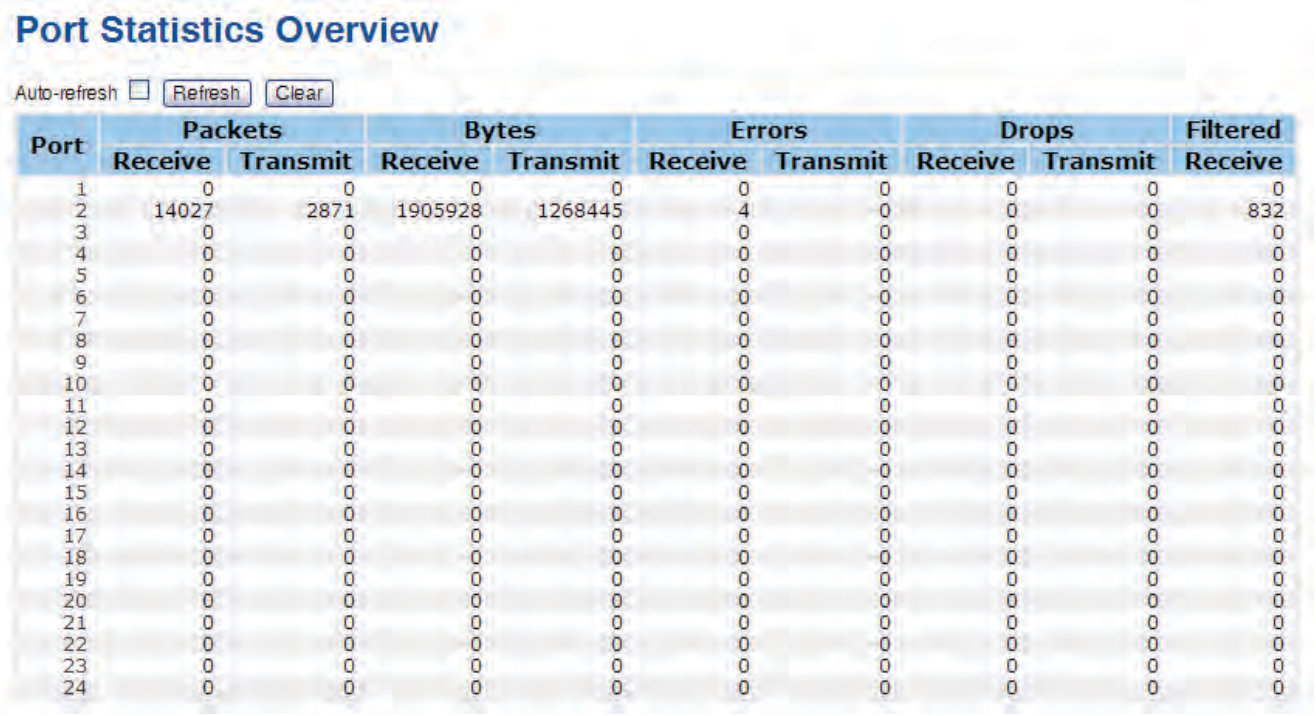
### System Log Information

The switch system log information is provided here.

| Label | Description |
|---|---|
| ID | The ID (>= 1) of the system log entry. |
| Level | The level of the system log entry. The following level types are supported:<br>Info: Information level of the system log.<br>Warning: Warning level of the system log.<br>Error: Error level of the system log.<br>All: All levels. |
| Time | The time of the system log entry. |
| Message | The MAC Address of this switch. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |
| Refresh | Updates the system log entries, starting from the current entry ID. |
| Clear | Flushes all system log entries. |
| \|<< | Updates the system log entries, starting from the first available entry ID. |
| << | Updates the system log entries, ending at the last entry currently displayed. |
| >> | Updates the system log entries, starting from the last entry currently displayed. |
| >>\| | Updates the system log entries, ending at the last available entry ID. |

### Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.



Port Statistics Overview

Auto-refresh ☐ Refresh Clear

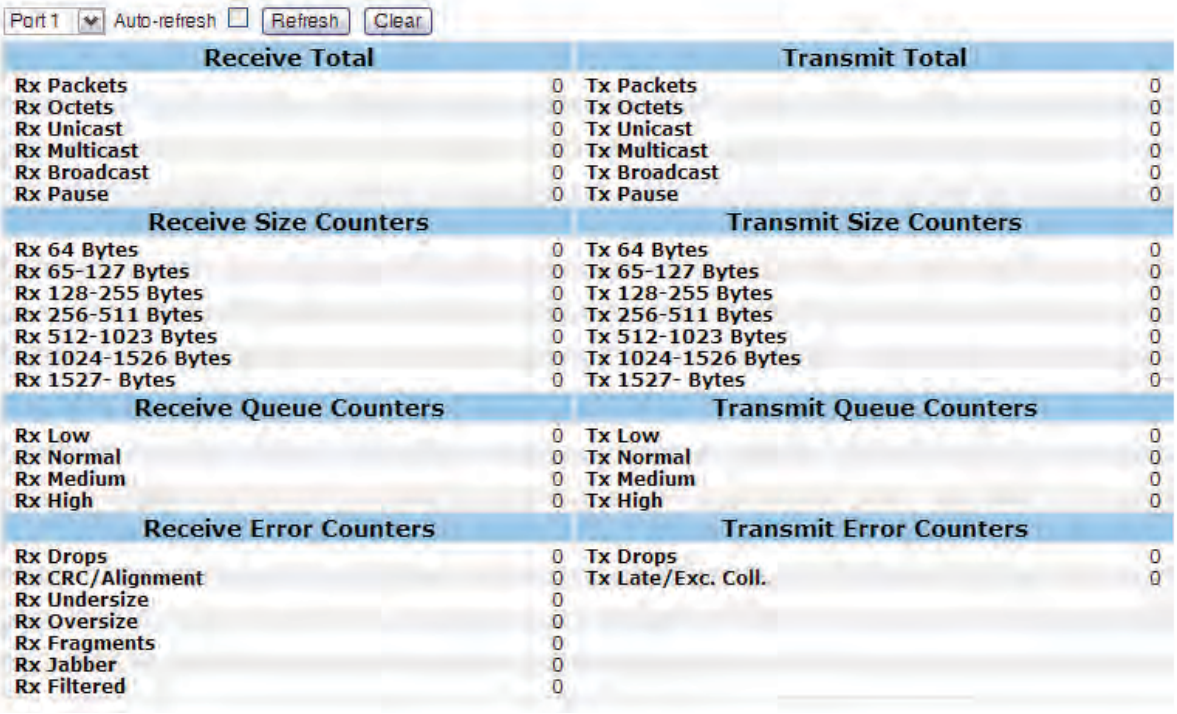
| Port | Packets | | Bytes | | Errors | | Drops | | Filtered |
|---|---|---|---|---|---|---|---|---|---|
| | Receive | Transmit | Receive | Transmit | Receive | Transmit | Receive | Transmit | Receive |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 14027 | 2871 | 1905928 | 1268445 | 4 | 0 | 0 | 0 | 832 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| Label | Description |
|---|---|
| Port | The logical port for the settings contained in the same row. |
| Packets | The number of received and transmitted packets per port. |
| Bytes | The number of received and transmitted bytes per port. |
| Errors | The number of frames received in error and the number of incomplete transmissions per port. |
| Drops | The number of frames discarded due to ingress or egress congestion. |
| Filtered | The number of received frames filtered by the forwarding process. |
| Auto-refresh | Check this box to enable an automatic refresh of the page at regular intervals. |
| Refresh | Updates the counters entries, starting from the current entry ID. |
| Clear | Flushes all counters entries. |

## Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.




*Detailed Statistics-Receive & Transmit Total*

| Label | Description |
|---|---|
| Rx and TX Packets | The number of received and transmitted (good and bad) packets. |
| Rx and TX Octets | The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. |
| Rx and TX Unicast | The number of received and transmitted (good and bad) unicast packets. |
| Rx and TX Multicast | The number of received and transmitted (good and bad) multicast packets. |
| Rx and TX Broadcast | The number of received and transmitted (good and bad) broadcast packets. |
| Rx and TX Pause | A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation. |
| Rx Drops | The number of frames dropped due to lack of receive buffers or egress congestion. |
| Rx CRC/ Alignment | The number of frames received with CRC or alignment errors. |
| Rx Undersize | The number of short 1 frames received with valid CRC. |
| Rx Oversize | The number of long 2 frames received with valid CRC. |
| Rx Fragments | The number of short 1 frames received with invalid CRC. |
| Rx Jabber | The number of long 2 frames received with invalid CRC. |
| Rx Filtered | The number of received frames filtered by the forwarding process. |
| TX Drops | The number of frames dropped due to output buffer congestion. |
| TX Late / Exc.Coll. | The number of frames dropped due to excessive or late collisions. |

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

### Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

After you press **Start**, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server::10.10.132.20

64 bytes from::10.10.132.20: icmp_seq=0, time=0ms

64 bytes from::10.10.132.20: icmp_seq=1, time=0ms

64 bytes from::10.10.132.20: icmp_seq=2, time=0ms

64 bytes from::10.10.132.20: icmp_seq=3, time=0ms

64 bytes from::10.10.132.20: icmp_seq=4, time=0ms

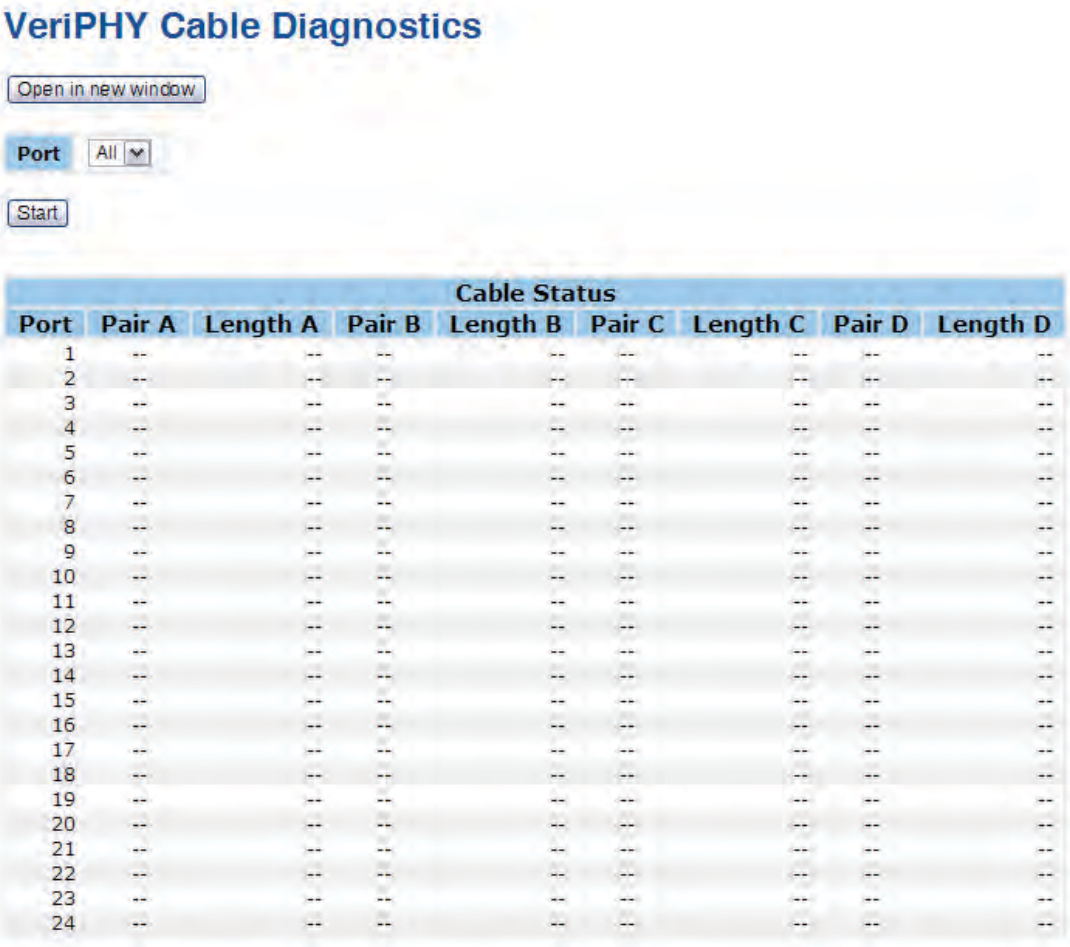
Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

| Label | Description |
|---|---|
| IP Address | The destination IP Address. |
| Ping Size | The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes. |

### VeriPHY

This page is used for running the VeriPHY Cable Diagnostics.




| Cable Status | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Port | Pair A | Length A | Pair B | Length B | Pair C | Length C | Pair D | Length D |
| 1 | -- | -- | -- | -- | -- | -- | -- | -- |
| 2 | -- | -- | -- | -- | -- | -- | -- | -- |
| 3 | -- | -- | -- | -- | -- | -- | -- | -- |
| 4 | -- | -- | -- | -- | -- | -- | -- | -- |
| 5 | -- | -- | -- | -- | -- | -- | -- | -- |
| 6 | -- | -- | -- | -- | -- | -- | -- | -- |
| 7 | -- | -- | -- | -- | -- | -- | -- | -- |
| 8 | -- | -- | -- | -- | -- | -- | -- | -- |
| 9 | -- | -- | -- | -- | -- | -- | -- | -- |
| 10 | -- | -- | -- | -- | -- | -- | -- | -- |
| 11 | -- | -- | -- | -- | -- | -- | -- | -- |
| 12 | -- | -- | -- | -- | -- | -- | -- | -- |
| 13 | -- | -- | -- | -- | -- | -- | -- | -- |
| 14 | -- | -- | -- | -- | -- | -- | -- | -- |
| 15 | -- | -- | -- | -- | -- | -- | -- | -- |
| 16 | -- | -- | -- | -- | -- | -- | -- | -- |
| 17 | -- | -- | -- | -- | -- | -- | -- | -- |
| 18 | -- | -- | -- | -- | -- | -- | -- | -- |
| 19 | -- | -- | -- | -- | -- | -- | -- | -- |
| 20 | -- | -- | -- | -- | -- | -- | -- | -- |
| 21 | -- | -- | -- | -- | -- | -- | -- | -- |
| 22 | -- | -- | -- | -- | -- | -- | -- | -- |
| 23 | -- | -- | -- | -- | -- | -- | -- | -- |
| 24 | -- | -- | -- | -- | -- | -- | -- | -- |

Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

| Label | Description |
|---|---|
| Port | The port where you are requesting VeriPHY Cable Diagnostics. |
| Cable Status | Port: Port number.<br>Pair: The status of the cable pair.<br>Length: The length (in meters) of the cable pair. |

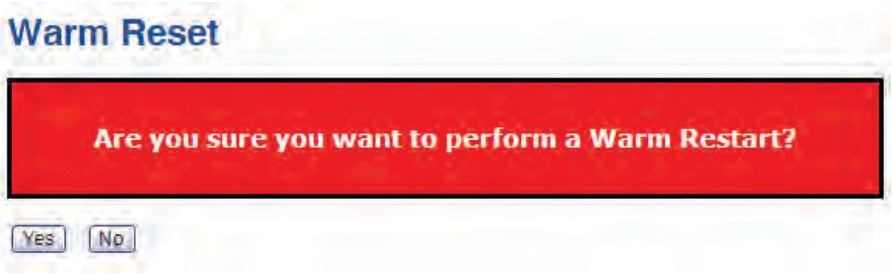
### Factory Defaults

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.

| Label | Description |
|---|---|
| Yes | Select to reset the configuration to Factory Defaults. |
| No | Select to return to the Port State page without resetting the configuration |

### System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices




| Label | Description |
|---|---|
| Yes | Select to reboot device. |
| No | Select to return to the Port State page without rebooting. |

# Command Line Interface Management

## About CLI Management

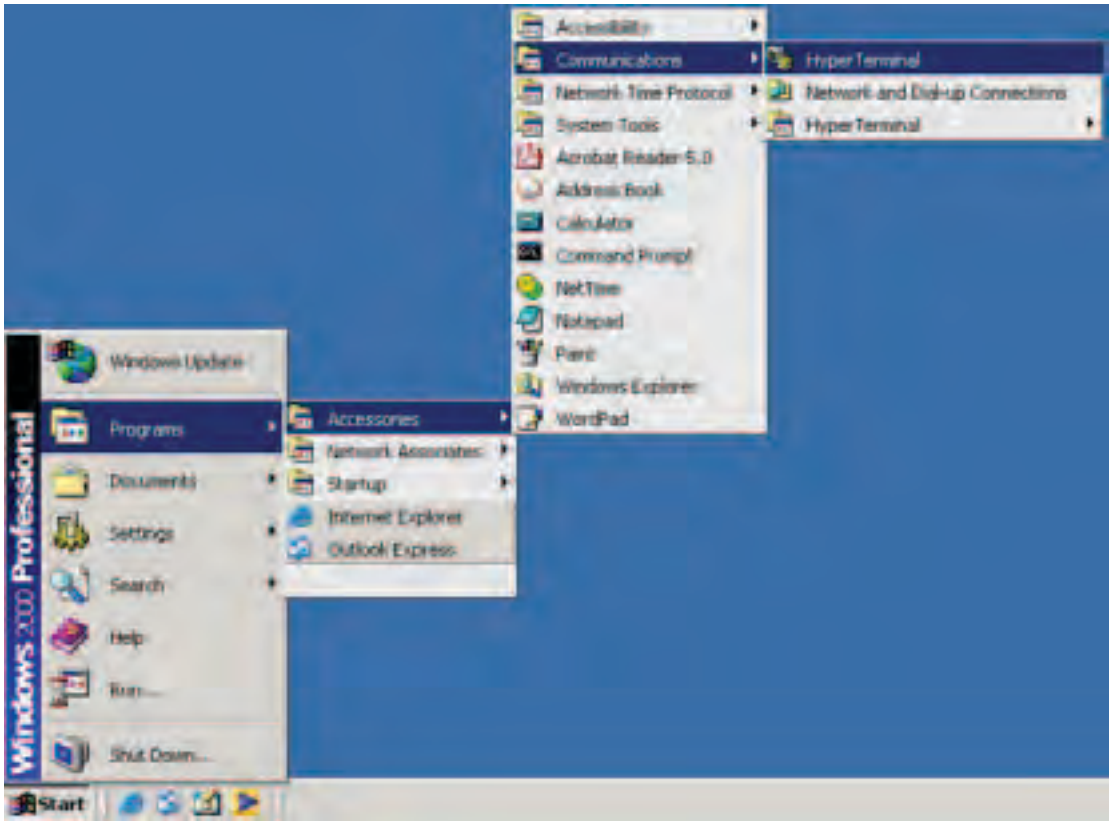
Besides WEB-based management, the CNGE24MS also support CLI management. You can use console or telnet to management switch by CLI.

### CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

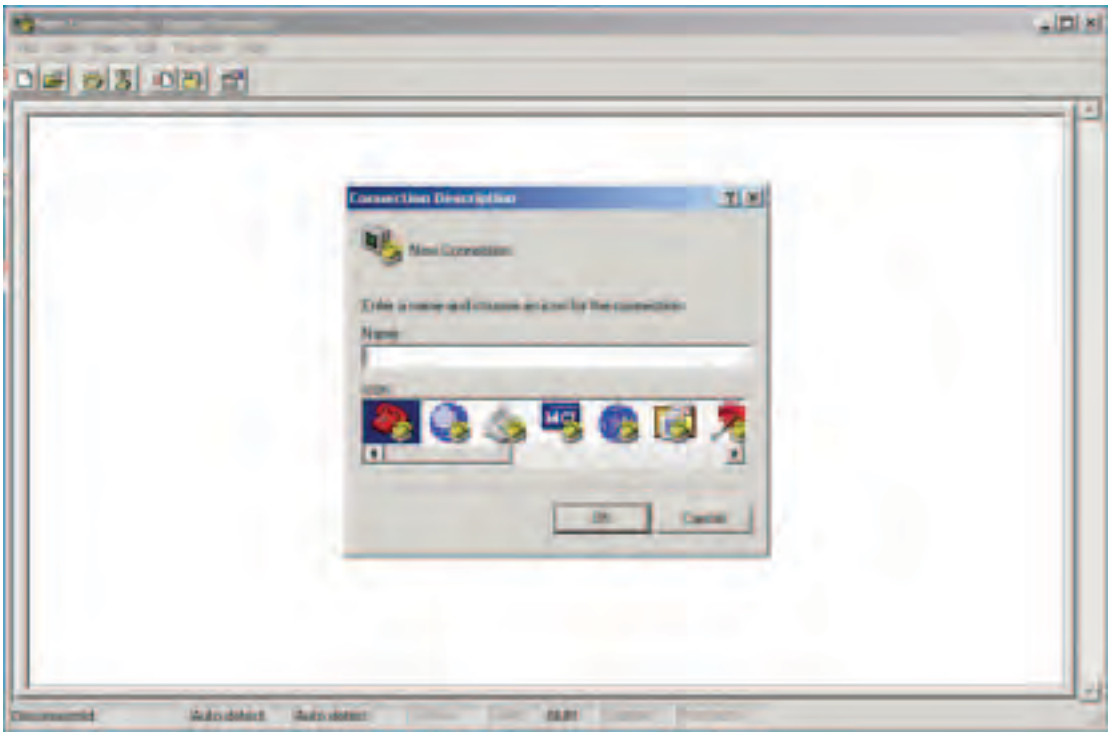
Before Configuring by RS-232 serial console, use an DB-9-M to DB-9-F cable to connect the switches' RS-232 Console port to your PC COM port.

Follow the steps below to access the console via RS-232 serial cable.

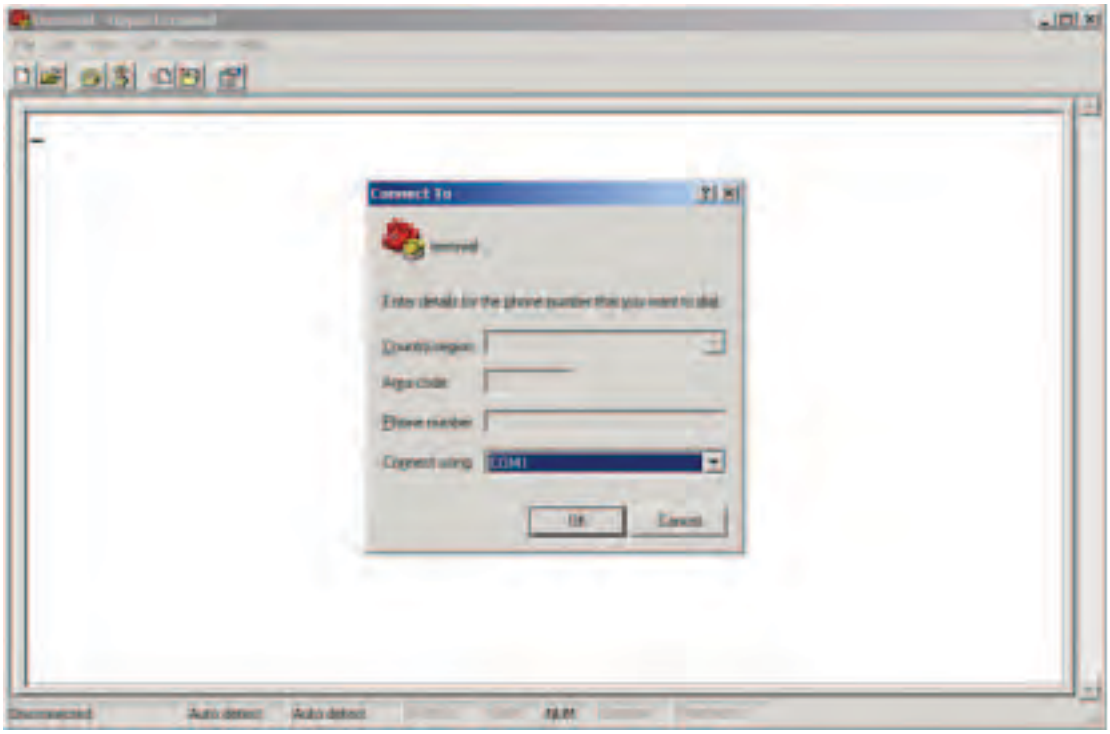
Step 1. From the Windows desktop, Select Start -> Programs -> Accessories -> Communications -> Hyper Terminal



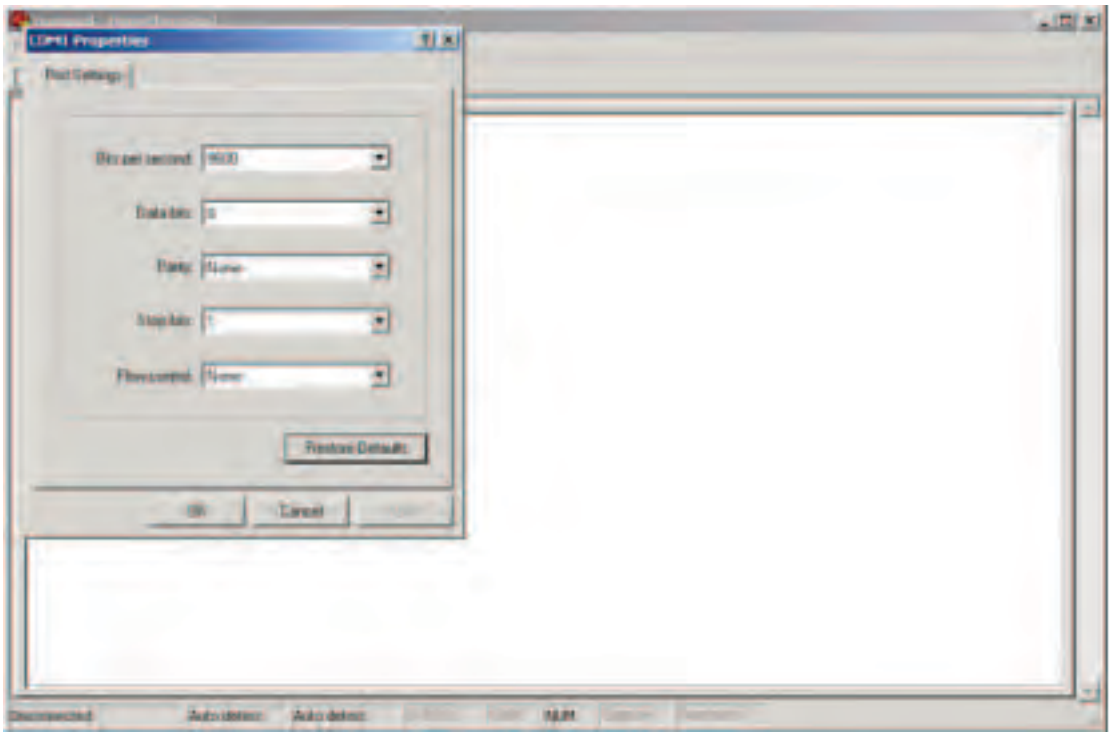

Step 2. Input a name for new connection



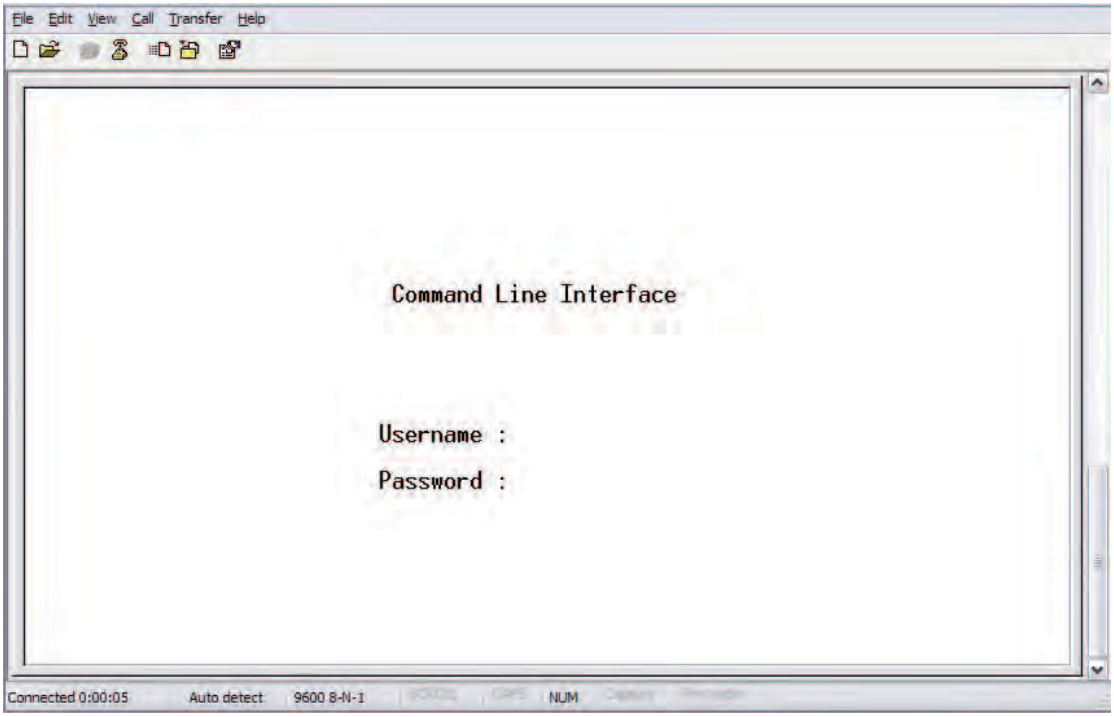
Step 3. Select to use COM port number



Step 4. The COM port properties setting, 115200 for baud rate, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (these are the same as the credentials for Web Browser), and then press **Enter**.



## CLI Management by Telnet

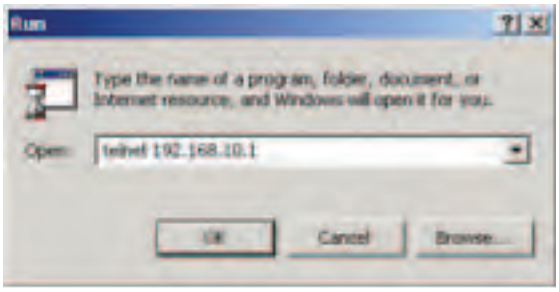
Users can use "TELNET" to configure the switches.

The default value is as below:

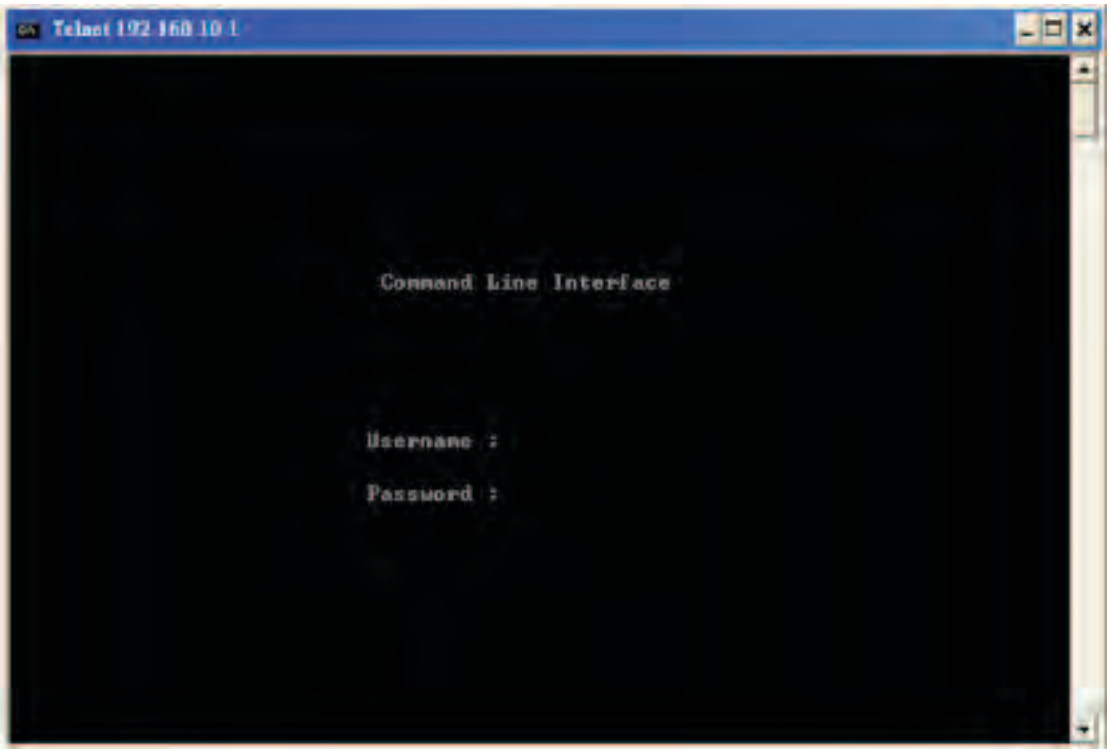
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.10.254
User Name: admin
Password: admin

Follow the steps below to access the console via Telnet.

Step 1. Telnet to the IP address of the switch from the Windows **Run** command (or from the MS-DOS prompt) as below.




Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), and then press **Enter**



Commander Groups

```
Command Groups:
---------------
System     : System settings and reset options
Syslog     : Syslog Server Configuration
IP         : IP configuration and Ping
Auth       : Authentication
Port       : Port management
Aggr       : Link Aggregation
LACP       : Link Aggregation Control Protocol
STP        : Spanning Tree Protocol
Dot1x      : IEEE 802.1X port authentication
IGMP       : Internet Group Management Protocol snooping
LLDP       : Link Layer Discovery Protocol
MAC        : MAC address table
VLAN       : Virtual LAN
PVLAN      : Private VLAN
QoS        : Quality of Service
ACL        : Access Control List
Mirror     : Port mirroring
Config     : Load/Save of configuration via TFTP
SNMP       : Simple Network Management Protocol
Firmware   : Download of firmware via TFTP
Fault      : Fault Alarm Configuration
```

System

| | |
|---|---|
| System> | Configuration [all] [<port_list>] |
| | Reboot |
| | Restore Default [keep_ip] |
| | Contact [<contact>] |
| | Name [<name>] |
| | Location [<location>] |
| | Description [<description>] |
| | Password <password> |
| | Username [<username>] |
| | Timezone [<offset>] |
| | Log [<log_id>] [all \| info \| warning \| error] [clear] |

## Syslog

| | |
|---|---|
| Syslog> | ServerConfiguration [<ip_addr>] |

## IP

| | |
|---|---|
| IP> | Configuration |
| | DHCP [enable \| disable] |
| | Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>] |
| | Ping <ip_addr_string> [<ping_length>] |
| | SNTP [<ip_addr_string>] |

## Auth

| | |
|---|---|
| Auth> | Configuration |
| | Timeout [<timeout>] |
| | Deadtime [<dead_time>] |
| | RADIUS [<server_index>] [enable \| disable] [<ip_addr_string>] [<secret>] [<server_port>] |
| | ACCT_RADIUS [<server_index>] [enable \| disable] [<ip_addr_string>] [<secret>] [<server_port>] |
| | Client [console \| telnet \| ssh \| web] [none \| local \| radius] [enable \| disable] |
| | Statistics [<server_index>] |

## Port

| | |
|---|---|
| Port> | Configuration [<port_list>] |
| | State [<port_list>] [enable \| disable] |
| | Mode [<port_list>] [10hdx \| 10fdx \| 100hdx \| 100fdx \| 1000fdx \| auto] |
| | Flow Control [<port_list>] [enable \| disable] |
| | MaxFrame [<port_list>] [<max_frame>] |
| | Power [<port_list>] [enable \| disable \| actiphy \| dynamic] |
| | Excessive [<port_list>] [discard \| restart] |
| | Statistics [<port_list>] [<command>] |
| | VeriPHY [<port_list>] |

## Aggr

| | |
|---|---|
| Aggr> | Configuration |
| | Add <port_list> [<aggr_id>] |
| | Delete <aggr_id> |
| | Lookup [<aggr_id>] |
| | Mode [smac \| dmac \| ip \| port] [enable \| disable] |

## LACP

| | |
|---|---|
| LACP> | Configuration [<port_list>] |
| | Mode [<port_list>] [enable \| disable] |
| | Key [<port_list>] [<key>] |
| | Role [<port_list>] [active \| passive] |
| | Status [<port_list>] |
| | Statistics [<port_list>] [clear] |

## STP

| | |
|---|---|
| STP> | Configuration |
| | Version [<stp_version>]<br>Non-certified release, v |
| | Txhold [<holdcount>]lt 15:15:15, Dec 6 2007 |
| | MaxAge [<max_age>] |
| | FwdDelay [<delay>] |
| | bpduFilter [enable \| disable] |
| | bpduGuard [enable \| disable] |
| | recovery [<timeout>] |
| | CName [<config-name>] [<integer>] |
| | Status [<msti>] [<port_list>] |
| | Msti Priority [<msti>] [<priority>] |
| | Msti Map [<msti>] [clear] |
| | Msti Add <msti> <vid> |
| | Port Configuration [<port_list>] |
| | Port Mode [<port_list>] [enable \| disable] |
| | Port Edge [<port_list>] [enable \| disable] |
| | Port AutoEdge [<port_list>] [enable \| disable] |
| | Port P2P [<port_list>] [enable \| disable \| auto] |
| | Port RestrictedRole [<port_list>] [enable \| disable] |
| | Port RestrictedTcn [<port_list>] [enable \| disable] |
| | Port bpduGuard [<port_list>] [enable \| disable] |
| | Port Statistics [<port_list>] |
| | Port Mcheck [<port_list>] |
| | Msti Port Configuration [<msti>] [<port_list>] |
| | Msti Port Cost [<msti>] [<port_list>] [<path_cost>] |
| | Msti Port Priority [<msti>] [<port_list>] [<priority>] |

## Dot1x

| | |
|---|---|
| Dot1x> | Configuration [<port_list>] |
| | Mode [enable \| disable] |
| | State [<port_list>] [macbased \| auto \| authorized \| unauthorized] |
| | Authenticate [<port_list>] [now] |
| | Reauthentication [enable \| disable] |
| | Period [<reauth_period>] |
| | Timeout [<eapol_timeout>] |
| | Statistics [<port_list>] [clear \| eapol \| radius] |
| | Clients [<port_list>] [all \| <client_cnt>] |
| | Agetime [<age_time>] |
| | Holdtime [<hold_time>] |

## IGMP

| | |
|---|---|
| IGMP> | Configuration [<port_list>] |
| | Mode [enable \| disable] |
| | State [<vid>] [enable \| disable] |
| | Querier [<vid>] [enable \| disable] |
| | Fastleave [<port_list>] [enable \| disable] |
| | Router [<port_list>] [enable \| disable] |
| | Flooding [enable \| disable] |
| | Groups [<vid>] |
| | Status [<vid>] |

## LLDP

| | |
|---|---|
| LLDP> | Configuration [<port_list>] |
| | Mode [<port_list>] [enable \| disable \| rx \| tx] |
| | Optional_TLV [<port_list>][port_descr \| sys_name \| sys_descr \| sys_capa \| mgmt_addr] [enable \| disable] |
| | Interval [<interval>] |
| | Hold [<hold>] |
| | Delay [<delay>] |
| | Reinit [<reinit>] |
| | Info [<port_list>] |
| | Statistics [<port_list>] [clear] |

## MAC

| | |
|---|---|
| MAC> | Configuration [<port_list>] |
| | Add <mac_addr> <port_list> [<vid>] |
| | Delete <mac_addr> [<vid>] |
| | Lookup <mac_addr> [<vid>] |
| | Agetime [<age_time>] |
| | Learning [<port_list>] [auto \| disable \| secure] |
| | Dump [<mac_max>] [<mac_addr>] [<vid>] |
| | Statistics [<port_list>] |
| | Flush |

## VLAN

| | |
|---|---|
| VLAN> | Configuration [<port_list>] |
| | Aware [<port_list>] [enable \| disable] |
| | PVID [<port_list>] [<vid> \| none] |
| | FrameType [<port_list>] [all \| tagged] |
| | Add <vid> [<port_list>] |
| | Delete <vid> |
| | Lookup [<vid>] |

## PVLAN

| | |
|---|---|
| PVLAN> | Configuration [<port_list>] |
| | Add <pvlan_id> [<port_list>] |
| | Delete <pvlan_id> |
| | Lookup [<pvlan_id>] |
| | Isolate [<port_list>] [enable \| disable] |

## QoS

| | |
|---|---|
| QoS> | Configuration [<port_list>] |
| | Classes [<class>] |
| | Default [<port_list>] [<class>] |
| | Tagprio [<port_list>] [<tag_prio>] |
| | QCL Port [<port_list>] [<qcl_id>] |
| | QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]<br>(etype <etype>) \|<br>(vid <vid>) \|<br>(port <udp_tcp_port>) \|<br>(dscp <dscp>) \|<br>(tos <tos_list>) \|<br>(tag_prio <tag_prio_list>)<br><class> |
| | QCL Delete <qcl_id> <qce_id> |
| | QCL Lookup [<qcl_id>] [<qce_id>] |
| | Mode [<port_list>] [strict \| weighted] |
| | Weight [<port_list>] [<class>] [<weight>] |
| | Rate Limiter [<port_list>] [enable \| disable] [<bit_rate>] |
| | Shaper [<port_list>] [enable \| disable] [<bit_rate>] |
| | Storm Unicast [enable \| disable] [<packet_rate>] |
| | Storm Multicast [enable \| disable] [<packet_rate>] |
| | Storm Broadcast [enable \| disable] [<packet_rate>] |

## ACL

| | |
|---|---|
| ACL> | Configuration [<port_list>] |
| | Action [<port_list>] [permit \| deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]<br>Policy [<port_list>] [<policy>] |
| | Rate [<rate_limiter_list>] [<packet_rate>] |
| | Add [<ace_id>] [<ace_id_next>] [switch \| (port <port>) \| (policy <policy>)]<br>[<vid>] [<tag_prio>] [<dmac_type>]<br>[(etype [<etype>] [<smac>] [<dmac>]) \|<br>(arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) \|<br>(ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) \|<br>(icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) \|<br>(udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) \|<br>(tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])]<br>[permit \| deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]<br>Delete <ace_id> |
| | Lookup [<ace_id>] |
| | Clear |

## Mirror

| | |
|---|---|
| Mirror> | Configuration [<port_list>] |
| | Port [<port> \| disable] |
| | Mode [<port_list>] [enable \| disable \| rx \| tx] |

## Config

| | |
|---|---|
| Config> | Save <ip_server> <file_name> |
| | Load <ip_server> <file_name> [check] |

## SNMP

| | |
|---|---|
| SNMP> | Trap Inform Retry Times [<retries>] |
| | Trap Probe Security Engine ID [enable \| disable] |
| | Trap Security Engine ID [<engineid>] |
| | Trap Security Name [<security_name>] |
| | Engine ID [<engineid>] |
| | Community Add <community> [<ip_addr>] [<ip_mask>] |
| | Community Delete <index> |
| | Community Lookup [<index>] |
| | User Add <engineid> <user_name> [MD5 \| SHA] [<auth_password>] [DES] [<priv_password>] |
| | User Delete <index> |
| | User Changekey <engineid> <user_name> <auth_password> [<priv_password>] |
| | User Lookup [<index>] |
| | Group Add <security_model> <security_name> <group_name> |
| | Group Delete <index> |
| | Group Lookup [<index>] |
| | View Add <view_name> [included \| excluded] <oid_subtree> |
| | View Delete <index> |
| | View Lookup [<index>] |
| | Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>] |
| | Access Delete <index> |
| | Access Lookup [<index>] |

## Firmware

| | |
|---|---|
| Firmware> | Load <ip_addr_string> <file_name> |

## Fault

| | |
|---|---|
| Fault> | Alarm PortLinkDown [<port_list>] [enable \| disable] |
| | Alarm PowerFailure [pwr1 \| pwr2 \| pwr3] [enable \| disable] |

# Technical Specifications

| ComNet Switch Model | CNGE24MS |
|---|---|
| **Physical Ports** | |
| Gigabit Combo port with 10/100/1000Base-T(X) and 100/1000Base-X SFP ports | 16 |
| 100/1000Base-X with SFP port | 8 |
| **Technology** | |
| Ethernet Standards | IEEE 802.3 for 10Base-T<br>IEEE 802.3u for 100Base-TX and 100Base-FX<br>IEEE 802.3ab for 1000Base-T<br>IEEE 802.z for 1000Base-X<br>IEEE 802.3x for Flow control<br>IEEE 802.3ad for LACP (Link Aggregation Control Protocol )<br>IEEE 802.1p for COS (Class of Service)<br>IEEE 802.1Q for VLAN Tagging<br>IEEE 802.1D for STP (Spanning Tree Protocol)<br>IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol)<br>IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol)<br>IEEE 802.1x for Authentication<br>IEEE 802.1AB for LLDP (Link Layer Discovery Protocol) |
| MAC Table | 8k |
| Priority Queues | 4 |
| Processing | Store-and-Forward |
| Switch Properties | Switching latency: 7 us<br>Switching bandwidth: 48Gbps<br>Max. Number of Available VLANs: 256<br>IGMP multicast groups: 128 for each VLAN<br>Port rate limiting: User Defined |
| Jumbo frame | Up to 9K Bytes |
| Security Features | IP Police security feature<br>Enable/disable ports, MAC based port security<br>Port based network access control (802.1x)<br>VLAN (802.1Q ) to segregate and secure network traffic<br>Radius centralized password management<br>SNMPv3 encrypted authentication and access security |

| | |
|---|---|
| Software Features | STP/RSTP/MSTP (IEEE 802.1D/w/s)<br>Redundant Ring (C-Ring) with recovery time <20ms over 250 units<br>TOS/Diffserv supported<br>Quality of Service (802.1p) for real-time traffic<br>VLAN (802.1Q) with VLAN tagging and GVRP supported<br>IGMP Snooping<br>IP-based bandwidth management<br>Application-based QoS management<br>DOS/DDOS auto prevention<br>Port configuration, status, statistics, monitoring, security<br>DHCP Client/Server |
| Network Redundancy | C-Ring<br>Legacy Ring<br>COM-Ring<br>STP<br>RSTP<br>MSTP |
| RS-232 Serial Console Port | RS-232 in DB9 connector with console cable. 115200bps, 8, N, 1 |
| **LED indicators** | |
| Power Indicator (PWR) | Green : Power indicator for AC and DC |
| Power-1 Indicator (PW1) | Green : Indicate Power-1 input |
| Power-2 Indicator (PW2) | Green : Indicate Power-2 input |
| Power-3 Indicator (PW3) | Green : Indicate Power-3 input |
| System Ready Indicator (STA) | Green : Indicates that the system ready. The LED is blinking when the system is upgrading firmware |
| Ring Master Indicator (R.M.) | Green : Indicates that the system is operating in C-Ring Master mode |
| C-Ring Indicator (Ring) | Green : Indicates that the system operating in C-Ring mode<br>Green Blinking : Indicates that the Ring is broken. |
| Fault Indicator (Fault) | Amber : Indicate unexpected event occurred |
| Sysem Runnig Indicator (RUN) | Green : System is operating continuously |
| Supervisor Login Indicator (RMT) | Green : System is accessed remotely |
| Reset To Default Running Indicator (DEF) | Green : System resets to default configuration |
| Ping Command To The Switch Indicator (Ping) | Green : System is processing “PING” request |
| 10/100/1000Base-T(X) RJ45 Port Indicator | Green for 1000Mbps Link/Act indicator<br>Amber for 10/100Mbps Link/Act indicator |

| | |
|---|---|
| 100/1000Base-X SFP Port Indicator | Green for port Link/Act. |
| **Fault contact** | |
| Relay | Relay output to carry capacity of 1A at 24VDC |
| **Power** | |
| Redundant Input power | 100~240VAC with power cord, dual 36 ~ 72VDC power inputs at 6-pin terminal block |
| Power consumption (Typ.) | 33 Watts |
| Overload current protection | Present |
| **Physical Characteristic** | |
| Enclosure | 19 inches rack mountable |
| Dimension (W x D x H) | 431 (W) x 342 (D) x 44 (H) mm |
| Weight (g) | 4.5 Kg |
| **Environmental** | |
| Storage Temperature | -40 to 85°C (-40 to 185°F) |
| Operating Temperature | -40 to 75°C (-40 to 158°F ) |
| Operating Humidity | 5% to 95% Non-condensing |
| **Regulatory approvals** | |
| EMI | FCC Part 15, CISPR (EN55022) class A |
| EMS | EN61000-4-2 (ESD)<br>EN61000-4-3 (RS),<br>EN61000-4-4 (EFT),<br>EN61000-4-5 (Surge),<br>EN61000-4-6 (CS),<br>EN61000-4-8,<br>EN61000-4-11 |
| Shock | IEC60068-2-27 |
| Free Fall | IEC60068-2-32 |
| Vibration | IEC60068-2-6 |
| Safety | EN60950-1 |
| Warranty | Lifetime |

**ComNet Customer Service**
Customer Care is ComNet Technology's global service center, where our professional staff is ready to answer your questions at any time.

Email ComNet Global Service Center: customercare@comnet.net

comnet
Communication Networks

3 CORPORATE DRIVE | DANBURY, CT 06810 | USA
T: 203.796.5300 | F: 203.796.5303 | TECH SUPPORT: 1.888.678.9427 | INFO@COMNET.NET

8 TURNBERRY PARK ROAD | GILDERSOME | MORLEY | LEEDS, UK LS27 7LE
T: +44 (0)113 307 6400 | F: +44 (0)113 253 7462 | INFO-EUROPE@COMNET.NET

© 2013 Communications Networks Corporation. All Rights Reserved. "ComNet" and the "ComNet Logo" are registered trademarks of Communication Networks, LLC.